НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«На правах рукопису»
УДК _____

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис)
“___” _____ 2019 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності: 113 «Прикладна математика»

на тему: «Диференціальні та лінійні властивості Фейстель-подібних безключових перетворень»

Виконала: студентка 6 курсу, групи ФІ-73мн
Євсюкова Яна Володимирівна
(підпис)

Керівник: к. т. н. Яковлєв С.В.
(підпис)

Рецензент:
(підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти: другий (магістерський) за освітньо–професійною програмою

Спеціальність: 113 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис)
«___»_____ 2019 р.

ЗАВДАННЯ
на магістерську дисертацію студентки

Євсюкової Яни Володимирівни

1. Тема дисертації: «Диференціальні та лінійні властивості Фейстель-подібних безключових перетворень», науковий керівник дисертації: к. т. н. Яковлєв С.В.,
затверджені наказом по університету від _____ р. № _____

2. Термін подання студентом дисертації _____

3. Об’єкт дослідження: інформаційні процеси в системах криптографічного захисту.

4. Предмет дослідження: моделі та методи диференціального та лінійного криптоаналізу ітеративних безключових симетричних схем блокових перетворень.

5. Перелік завдань, які потрібно розробити:

- для трираундової безключової схеми CLEFIA із певними додатковими умовами одержати аналітичні оцінки диференціальної рівномірності через відповідні параметри її раундових функцій;
- для трираундової безключової схеми CLEFIA із певними додатковими умовами одержати аналітичні оцінки лінійних потенціалів через відповідні параметри її раундових функцій;
- порівняти криптографічні властивості трираундової безключової схеми CLEFIA та інших схем ітеративних блокових перетворень;

6. Орієнтовний перелік ілюстративного матеріалу:

- ілюстрації до структур і процесів в технологіях, розглянутих в даній роботі;
- перелік формул, що характеризують диференціальну рівномірність та лінійні потенціали;

7. Орієнтовний перелік публікацій відсутній.

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Ознайомлення з літературою на визначену область легкої криптографії, що буде розглянута в дослідницькій роботі	листопад 2017 р.	Виконаний
2	Конкретизація проблемних аспектів обраної області легкої криптографії	січень 2018 р.	Виконаний

	Визначення, яка саме схема буде досліджуватися, та підготовка звіту на цю тему	квітень 2018 р.	Виконаний
3	Формулювання теми магістерської дисертації	вересень 2018 р.	Виконаний
4	Постановка задач дослідницької роботи та переліку потенційних методів для їх виконання	листопад 2018 р.	Виконаний
5	Аналіз та опис поняття легковагова криптографія, визначення основних принципи використання даного напряму криптографії. Формування відповідних звітностей	січень 2019 р.	Виконаний
6	Побудова аналітичних оцінок диференціальної рівномірності та лінійних потенціалів для схеми CLEFIA через відповідні параметри її раундових функцій.	березень 2019 р.	Виконаний
7	Порівняльний аналіз диференціальної рівномірності та лінійних потенціалів для схеми CLEFIA та інших схем ітеративних блокових перетворень.	квітень 2019 р.	Виконаний

Студент _____ Євсюкова Я. В.
(підпис)

Науковий керівник дисертації _____ Яковлєв С. В.
(підпис)

РЕФЕРАТ

Кваліфікаційна робота містить: 84 стор., 3 рисунки, 36 джерел.

У сучасному світі виникла проблема забезпечення захисту криптографічними методами приладів, обладнаних дуже обмеженою потужністю і пам'яттю. Рішенням даної проблеми стало виникнення нового напряму – легковагова криптографія.

Одним із методів створення легкого шифру є використання великих S-блоків, створенних з більш малих. Схема CLEFIA блокового перетворення є одним з аналогів популярної схеми Фейстеля, що можна використовувати для побудови S-блоків. У даній роботі одержано аналітичні оцінки для диференціальної рівномірності та лінійних потенціалів трираундової безключової схеми CLEFIA через відповідні параметри її раундових функцій. Також проведено порівняльний аналіз криптографічних властиво стей схеми CLEFIA з іншими схемами криптографічних безключових перетворень.

БЛОКОВІ ШИФРИ, CLEFIA, ЛЕГКА КРИПТОГРАФІЯ, S-БЛОКИ

ABSTRACT

Qualifying work includes: 84 p., 3 pictures, 36 sources.

In today's world there is a problem of cryptographic protection of device equipped with very limited power and memory. The solution was the emergence of a new trend - lightweight cryptography.

One method of creating a light cipher is to use large S-Boxes which were made from small S-Boxes. Block encryption scheme CLEFIA is one of the analog of wide known Feistel scheme. This scheme we can use for creating a new S-Box. We present analytic bounds for differential probabilities and linear potentials of three-round keyless scheme CLEFIA, expressed with corresponding parameters of its round mappings. Also, we compare cryptographic properties of scheme CLEFIA with other schemes of cryptographic transformations.

BLOCK CIPHERS, CLEFIA, LIGHTWEIGHT CRYPTOGRAPHY, S-BOXES

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

$\oplus$ — операція побітового додавання

V_n — простір двійкових векторів довжини n:

$a \to b$ — диференціал (a,b) деякої функції

$\delta_F(a,b)$ — диференціальна рівномірність функції F

$\mathcal{L}(F)$ — нелінійність функції F

ВСТУП

Актуальність дослідження. У наш час відбувається глобальна трансформація індустріального суспільства в постіндустріальне або інформаційне. Це стало можливим завдяки швидкому розвитку та впровадженню сучасних інформаційно-комунікаційних технологій. Масове використання комп'ютерних мереж та електронних комунікацій значно розширює можливості для обміну інформацією між користувачами. У світовому інформаційному просторі та інформаційних просторах держав вирішуються складні завдання переходу до використання систем електронних документів та електронного документообігу, електронної торгівлі, електронних банківських систем, електронних баз тощо. Електроні системи знаходять широке впровадження в науці, освіті, управлінні державою тощо. Використання Інтернету для електронного ведення бізнесу значно збільшує риск несанкціонованих впливів на фінансові документи та іншу важливу інформацію. Технологічний прогрес не стоїть на місці. Вже створено новий напрямок на підвищення ефективності економіки за рахунок автоматизації процесів у різних сферах діяльності і виключення з них людини. Даний напрямок має назву Інтернет речей. Інтернет речей є ключовим словом у сучасному світі. Пристрої, які беруть участь в даному напрямку, обладнані дуже обмеженою потужністю і пам'яттю. Через це виникає проблема використання класичної криптографії на даних пристроях. Таким чином, щоб задовольнити вимоги безпеки Інтернету речей, виникла так звана легка криптографія. Тому у наш час стає дуже важливим завданням вивчення даного напряму криптографії та виявлення певних властивостей та закономірностей елементів криптографічних систем задля покращення вже існуючих легких шифрів або створення нових.

Ще одним важливим напрямком криптографії є вивчення та

дослідження схем безключового перетворення. Дана тема сьогодні також є досить актуальною, оскільки відомо, що зі схем такого типу створюються складові частини шифрів а також геш-функції, котрі являють собою невід'ємну частину криптографії.

Диференціальний [3] та лінійний [4] криптоаналіз є двома потужними методами аналізу симетричних блокових шифрів. Стійкість до даних методів є обов'язковою вимогою для усіх сучасних алгоритмів шифрування. Природний спосіб оцінювання стійкості шифрів до диференціального та лінійного криптоаналізу полягає у дослідженні максимальних ймовірностей диференціалів (потенціалів лінійних наближень) шифруючих перетворень, усереднених по усіх можливих ключах. Однак цей підхід не застосовний для випадку ітеративних безключових перетворень, які останнім часом широко використовуються у легкій криптографії для побудови надійних та ефективно обчислюваних нелінійних відображень (наприклад, S-блоків). У цьому випадку для забезпечення стійкості необхідно гарантувати невеликі значення диференціальних імовірностей та лінійних потенціалів перетворення в цілому. Встановлювати ці параметри шляхом безпосередньої перевірки можна лише для перетворень із невеликим розміром блоку. Тому дуже слушними стають аналітичні методи оцінювання криптографічних параметрів ітеративних безключових перетворень через відповідні параметри їх складових елементів.

Метою дослідження є аналіз нових підходів до оцінювання теоретичної (доказової) стійкості схем ітеративних блокових перетворень до диференціального та лінійного криптоаналізу та застосування їх до оцінювання стійкості схем блокового шифрування, що дозволить значно розширити клас надійних шифрів та сприятиме підвищенню рівня та якості інформаційної безпеки.

Задачею дослідження є оцінювання криптографічних властивостей схеми CLEFIA.

Досягнення поставленої мети передбачає наступні **завдання**

дослідження, які були виконані в роботі:

1) вивчити поняття легковагова криптографія, визначити основні принципи використання даного напряму криптографії;

2) вивчити основні принципи переходу від ключових схем криптографічних перетворень до безключових.

3) для трираундової безключової схеми CLEFIA із певними додатковими умовами одержати аналітичні оцінки диференціальної рівномірності через відповідні параметри її раундових функцій;

4) для трираундової безключової схеми CLEFIA із певними додатковими умовами одержати аналітичні оцінки лінійних потенціалів через відповідні параметри її раундових функцій;

5) порівняти криптографічні властивості трираундової безключової схеми CLEFIA та інших схем ітеративних блокових перетворень;

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є моделі та методи диференціального та лінійного криптоаналізу ітеративних безключових симетричних схем блокових перетворень.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи лінійної та абстрактної алгебри, математичної статистики, комбінаторного аналізу, теорії кодування, теорії складності алгоритмів.

Наукова новизна. В роботі отримані наступні наукові результати.

1) одержано аналітичні оцінки диференціальної рівнмірності для ітеративних криптографічних блокових перетворень: трираундової безключової схеми CLEFIA;

2) одержано аналітичні оцінки лінійних потенціалів для ітеративних криптографічних блокових перетворень: трираундової безключової схеми CLEFIA.

Практичне значення. У результаті виконання дипломної роботи одержані аналітичні оцінки диференціальної рівномірності та лінійних

потенціалів для трираундової безключової схеми CLEFIA. Результати даної роботи позволяють підвищити ефективність методів аналізу та синтезу алгоритмів легкої криптографії.

1 ЛЕГКОВАГОВА КРИПТОГРАФІЯ ТА ІТЕРАТИВНІ БЛОКОВІ ПЕРЕТВОРЕННЯ

В даному розділі йдеться мова про основні поняття легковагової криптографії. Також розглядаються основні терміни та позначення для диференціального та лінійного криптоаналізу ітеративних схем блокових перетворень.

1.1 Легка криптографія в Інтернеті речей

Інтернет речей (Internet of Things, або IoT) виявився новим обговоренням у сфері досліджень і практичної реалізації в останні роки. IoT – це модель, яка включає звичайні об'єкти з можливістю відчувати та зв'язуватися з іншими пристроями, використовуючи Інтернет. Оскільки широкосмуговий Інтернет зараз загалом доступний і його вартість підключення також зменшується, до нього підключаються більше гаджетів і датчиків. Такі умови забезпечують відповідну основу для зростання IoT. Існує багато складнощів навколо IoT, оскільки ми хочемо мати доступ до кожного об'єкту з будь-якої точки світу. Витончені фішки та сенсори вбудовані у фізичні речі, які оточують нас, кожна з яких передає цінні дані. Процес обміну такою великою кількістю даних починається з самих пристроїв, які повинні надійно спілкуватися з платформою IoT. Ця платформа об'єднує дані з багатьох пристроїв і застосовує аналітику для обміну найбільш цінними даними з додатками. IoT переводить звичайний інтернет, сенсорну мережу та мобільну мережу на інший рівень, оскільки кожна річ буде підключена до Інтернету. Питання, яке має бути розглянуто, – це питання, що стосуються

конфіденційності, цілісності та автентичності даних, які виникатимуть через безпеку та конфіденційність.

З плином часу все більше і більше пристроїв підключаються до Інтернету. Будинки незабаром будуть оснащені смарт-замками, персональний комп'ютер, ноутбуки, планшети, смартфони, смарт-телевізори, відеоігри, навіть холодильники і кондиціонери мають можливість комунікувати через Інтернет. Ця тенденція поширюється назовні, і, за підрахунками, до 2020 року буде більше 50 мільярдів об'єктів, підключених до Інтернету. Це оцінює, що для кожної людини на Землі буде 6,6 об'єктів онлайн. Земля буде покрита мільйонами датчиків, які збирають інформацію з фізичних об'єктів і завантажуватимуть її в Інтернет. Зростаючий інтерес до використання IoT проглядається в системі автоматизації будівель, в галузях охорони здоров'я, гірничодобувному виробництві та інших сферах життя.

Передбачається, що застосування IoT ще на ранній стадії, але починає швидко розвиватися. Маючи багато додатків, щоб адаптувати технологію з намірами зробити внесок у зростання економіки, медичної установи, транспорту та покращити спосіб життя для громадськості, IoT повинна надавати належну безпеку своїм даним, щоб заохотити процес адаптації.

1.1.1 Загрози безпеці в Інтернеті речей

З точки зору високого рівня, IoT складається з трьох компонентів, а саме: Hardware, Middleware і Presentation. Hardware засоби складаються з датчиків і приводів, Middleware забезпечує зберігання і обчислювальні засоби, а Presentation надає засоби інтерпретації, доступні на різних платформах. Неможливо обробляти дані, зібрані з мільярдів датчиків,

тому пропонуються рішення, які мають на увазі контекстне програмне забезпечення, щоб допомогти датчику визначити найбільш важливі дані для обробки. По суті, архітектура IoT не пропонує достатньої маржі для виконання необхідних дій, пов'язаних з процесом аутентифікації та цілісності даних. Пристрої в IoT, такі як RFID, є сумнівними для досягнення фундаментальних вимог процесу аутентифікації, що включає постійне спілкування з серверами і обмін повідомленнями з вузлами.

IoT є надзвичайно відкритим для атак , тому що існує шанс фізичної атаки на його компоненти, оскільки вони залишаються без нагляду протягом тривалого часу. Завдяки бездротовому засобу зв'язку, прослуховування є надзвичайно простим. Нарешті, складові IoT мають низьку компетентність щодо енергії, з якою вони експлуатуються, а також з точки зору обчислювальних можливостей. Впровадження звичайних обчислювально дорогих алгоритмів безпеки призведе до перешкод на продуктивності пристроїв, обмежених енергією. [26]

Найбільша загроза безпеки IoT-систем від традиційних IT-систем полягає в тому, що навіть використання пристроїв для збору даних з реального світу може стати об'єктом кібератак. Наприклад, метою застосування IoT до заводу є значне підвищення продуктивності та ремонтопридатності шляхом збору даних з великої кількості датчиків, встановлених у виробничому обладнанні, шляхом аналізу його та здійснення автономного управління в реальному часі. Якщо дані датчиків повинні бути фальсифіковані під час цього процесу, будуть викликані неправильні результати аналізу і виникне помилковий контроль через такий випадок, що призведе до великого пошкодження. Більше того, оскільки дані вимірювань та команди керування є комерційною таємницею, пов'язаною з ноу-хау виробництва та управління, запобігання витоків також важливо з точки зору конкурентоспроможності. Навіть якщо в даний час не існує жодних проблем, необхідно розглянути вплив загроз, які можуть стати очевидними в майбутньому.

Було запропоновано багато рішень для бездротових сенсорних

мереж, які розглядають датчик як частину інтернету, з'єднаного через вузли. Проте в IoT самі вузли датчиків розглядаються як інтернет-вузли, що робить процес аутентифікації ще більш значним. Цілісність даних також стає життєво важливою і вимагає особливої уваги до збереження її надійності. [27]

1.2 Необхідність розвитку легкої криптографії

Нещодавно дослідження HP показує, що 70% пристроїв в IoT є вразливими до атак. Атака може бути виконана шляхом відчуття зв'язку між двома вузлами, яка відома як атака «людина в середині». Жодного надійного рішення не було запропоновано для задоволення таких нападів. Однак шифрування може призвести до мінімізації кількості завданої шкоди цілісності даних. Щоб забезпечити уніфікацію даних, поки вони зберігаються на середньому пристрої, а також під час передачі, необхідно мати механізм безпеки. Були розроблені різні криптографічні алгоритми, які стосуються цього питання, але їх використання в IoT викликає сумніви, оскільки апаратні засоби, які ми маємо в IoT, не підходять для реалізації дорогих алгоритмів шифрування. А реалізація відомих сучасних криптографічних алгоритмів є дуже грошозатратним заходом [26]. В даний час в сучасній криптографії існують такі проблеми:

1) Обмеженість числа робочих схем. На відміну від алгоритмів класичної криптографії, які можуть бути створені в необмеженій кількості шляхом комбінування різних елементарних перетворень, кожна «сучасна» схема базується на певній «нездійсненним» завданню. Як наслідок, кількість робочих схем криптографії з відкритим ключем досить невелика;

2) Постійна «інфляція» розміру блоків даних і ключів, обумовлена

прогресом математики та обчислювальної техніки. Так, якщо в момент створення криптосистеми RSA вважався достатнім розмір чисел в 512 біт, то зараз рекомендується не менше 4 Кбіт. Іншими словами, «безпечний» розмір чисел в RSA виріс практично на порядок; схожа картина спостерігається і для інших схем, тоді як в традиційній криптографії цей розмір збільшився всього вдвічі;

3) Потенційна ненадійність базису. В даний час теорією обчислювальної складності досліджується питання про можливість вирішення завдань даного типу за поліноміальний час (гіпотеза P = NP). В рамках теорії вже доведено зв'язок більшості використовуваних обчислювально складних задач з іншими аналогічними завданнями. Це означає, що, якщо буде зламана хоча б одна сучасна криптосистема, багато інших також не встоять;

4) Відсутність далекої перспективи. З розвитком технологій і збільшенням обчислювальних потужностей, подальше збільшення розміру блоків даних і довжини ключа, призведе до того, що шифрування втратить своєї легкості використання і можливо сучасна криптографія просто прийде в непридатність через те, що рішення «неможливих» завдань стане можливим. Прикладом цього можна привести квантовий комп'ютер [28].

Тому виникло питання у необхідності зробити компроміс для виконання вимог безпеки з низькими обчислювальними витратами. [26]

Це стало причиною виникнення нового напряму інформаційного захисту – легка криптографія. Легка криптографія може бути реалізована за нижчих витрат і з меншим енергоспоживанням у порівнянні зі звичайною криптографією.

Потреба в легкій криптографії широко обговорюється, а також висвітлюються недоліки IoT з точки зору обмежених пристроїв. Насправді існують деякі легкі алгоритми криптографії, які не завжди використовують компроміси ефективності безпеки. Серед блокових шифрів, потокових шифрів і геш-функцій, шифри блоків показали значно

кращі показники. [26]

Кожен дизайнер легкої криптографії повинен впоратися з компромісом між безпекою, витратами та продуктивністю. Для блочних шифрів довжина ключа забезпечує компроміс у вартості безпеки, тоді як кількість раундів забезпечує компроміс між продуктивністю безпеки та апаратною архітектурою співвідношення витрат та продуктивності (див. Малюнок 2.1). Як правило, будь-які дві з трьох цілей проектування – безпека і низькі витрати, безпека і продуктивність, або низькі витрати і продуктивність – можуть бути легко оптимізовані, тоді як дуже важко оптимізувати всі три цілі проектування одночасно. Наприклад, безпечна і високопродуктивна апаратна реалізація може бути досягнута за допомогою конвеєрної архітектури, яка також включає багато контрзаходів проти атак з боку каналу. Отримана конструкція мала б високі вимоги до області, що корелює з високими витратами. З іншого боку, можна розробити безпечну і дешеву апаратну реалізацію з недоліком обмеженої продуктивності [29].

Для легких криптографічних технологій запропоновано різні методи. Деякі шукають легку вагу з точки зору розміру апаратної реалізації та енергоспоживання, в той час як інші шукають її з точки зору необхідного розміру пам'яті вбудованого програмного забезпечення. Кожен метод оптимізований відповідно до різних показників продуктивності [30].

Взагалі кажучи, існують три підходи для забезпечення криптографічних примітивів для надзвичайно легких додатків:

1) Оптимізовані недорогі реалізації для стандартизованих і надійних алгоритмів.

2) Трохи змінений добре вивчений і надійний шифр.

3) Розробити нові шифри з метою зниження витрат на реалізацію обладнання.

Для легкої криптографії необхідні наступні чинники.

– Розмір (розмір схеми, розміри ROM/RAM);

– Потужність;

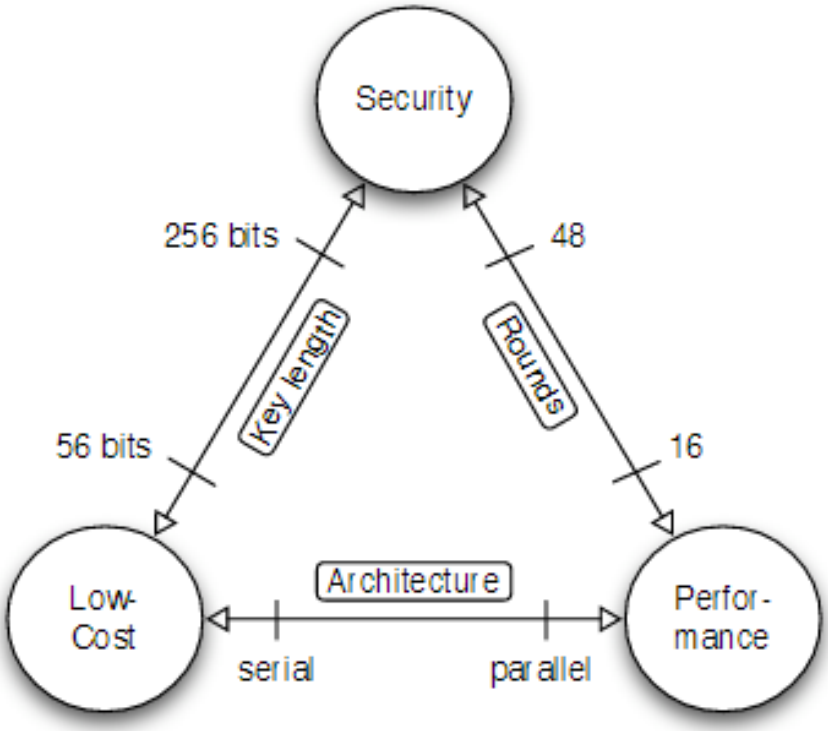

Рисунок 1.1 – Розробка компромісу для легкої криптографії [29]

– Споживання енергії;

– Швидкість обробки (пропускна здатність, затримка).

Першим фактором, що визначає можливість реалізації в пристрої, є розмір. Потужність особливо важлива для RFID та енергозберігаючих пристроїв, а споживання енергії є важливим з акумуляторними пристроями. Висока пропускна здатність необхідна для пристроїв з великими передачами даних, таких як камера або датчик вібрації, а низька затримка важлива для обробки в режимі реального часу системою управління автомобілем тощо.

Оскільки потужність значно залежить від апаратних засобів, таких як розмір схеми або використовуваний процесор, розмір стає опорною точкою для легкості методу шифрування, а також для живлення. Споживання енергії залежить від швидкості обробки через час виконання, тому кількість обчислень, що визначають швидкість обробки, стає індексом легкості. Пропускна здатність значно залежить від

можливості паралельної обробки.

Що стосується безпеки, оскільки шифрування є технологічною точкою походження загальної безпеки системи, то легка криптографія повинна прийняти метод, який оцінюється як такий, що має достатній рівень безпеки сучасної криптографії. Навіть коли довжина блоку та/або довжина секретного ключа встановлюються коротше, ніж для стандартної криптографії, шляхом визначення пріоритету простоти реалізації (наприклад, через 64-розрядний блок і 80-бітний секретний ключ), вона все ще потрібна для правильного застосовують перевірений метод [27].

Легковагова криптографія заснована як на симетричній криптографії, так і на асиметричній. Однак зазвичай використовують принципи симетричної криптографії, оскільки в області криптографії з відкритим ключем питання пошуку оптимального легковагового алгоритму, порівняного по надійності з RSA або з алгоритмом, заснованим на еліптичних кривих, залишається відкритим, так як асиметричні системи більш вимогливі до часових ресурсів, ніж симетричні. Однак деякі досягнення в даній сфері існують.

Що стосується симетричної криптографії, то легка криптографія використовує як блокові, так і потокові алгоритми. Класичними потоковими алгоритмами є: алгоритм потокового шифрування MICKEY [16], симетричний алгоритм синхронного потокового шифрування Trivium [17], алгоритм потокового шифрування GRAIN [15] та інші. Найчастіше потокові шифри дуже незручні для легковагової реалізації призначеної для обробки дуже невеликих масивів інформації, тому що мають, як правило, порівняно великий час ініціалізації. Крім того більшість поточних шифрів вимагають великої кількості пам'яті для запису свого внутрішнього стану. Отже, ці шифри не можуть забезпечити ефективне шифрування невеликих обсягів даних, що найбільш характерно для вбудованих систем.

В області блокового шифрування найбільш популярними

легковаговими алгоритмами вважаються CLEFIA [13] та PRESENT [7]. Обидва алгоритми відомі ще з 2007 року. У 2012 році організації ISO та IEC включили алгоритми CLEFIA [13] та PRESENT [7] до міжнародного стандарту легковагового шифрування ISO/IEC 29192-2:2012. У лютому 2014 року стало відомо про розробку нового легковагового блокового шифру Halka. Його головна відмінність – використання восьмибітних S-блоків, у той час як більшість інших блокових алгоритмів з легковаговими властивостями використовують чотирьохбітні S-блоки. Використання восьмибітних S-блоків гарантує більш високу криптостійкість. Іншими відомими легковаговими блоковими шифрами є HIGHT [8], LBlock [9], TWINE [10], SIMON та сімейство SPECK [11], TEA та DESL [12]. Також існують досить молоді алгоритми KATAN та KTANTAN [14], а також MIBS або mCrypton, які ще не достатньо добре досліджені.

Що стосується легковагової геш-функції, то на сьогоднішній день відомі такі механізми легковагової геш-функції, як S-Quark та D-Quark, PHOTON та SPONGENT. Усі ці алгоритми засновані на принципу криптографічної губки, що позволяє оперувати з даними довільної довжини як на вході, так і на виході алгоритму.

Однак деякі з алгоритмів в силу індивідуальних особливостей не можуть застосовуватися повсюдно. Наприклад алгоритм Trivium [17] потребує для своєї реалізації на кристалі площу, яка в півтора рази перевищує усі допустимі межі, алгоритм GRAIN [15] в легковаговій версії успішно піддається атаці на зв'язаних ключах, а алгоритм MICKEY [16] достатньо стійкий не до всіх видів атак, і багато спеціалістів недостатньо впевнені в його надійності.

Серед блокових шифрів ситуація трохи краща. Шифр DESL [12], розроблений на основі відомого алгоритму DES, є вдалим рішенням у малоресурсній криптографії завдяки тому, що останній уже розроблювався з врахуванням апаратної реалізації. Авторами DESL [12] доведено, що зміни, внесені в алгоритм при його адаптації не впливають

на його стійкість до атак в рамках диференціального та лінійного криптоаналізу. Єдиним серйозним недоліком є ключ довжиною всього у 56 біт – такий ключ розкривається на потужній багатопроцесорній системі повним перебором упродовж декількох діб.

1.2.1 Використання S-блоків у легковаговій криптографії

Шеннон був першим, хто формалізував ідеї перемішування та розсіювання у вигляді двох властивостей при проектуванні захищеного шифру. На практиці майже всі блокові шифри засновані на наступних операціях перемішування та розсіювання. У блокових шифрів, перемішування часто ототожнюється з рівнем заміни, тоді як розсіювання зазвичай ототожнюється з перестановкою або з рівнем «змішування». Насправді не завжди легко відокремити і ідентифікувати компоненти, які сприяють до перемішування або розсіювання.

Деякі шифри використовують арифметичні операції для забезпечення перемішування та розсіювання, але це може значно збільшити площу і споживання енергії. Найбільш поширений метод досягнення перемішування заснований на S-блоках. Невелика зміна на вході в S-блоці призводить до складної зміни в вихідному сигналі. Для того, щоб швидко поширити ці вихідні зміни по всім станам, повинен бути застосований рівень розсіювання. Класичний спосіб зробити це полягає у використанні бітової перестановки. В апаратних засобах, бітові перестановки можуть бути реалізовані з допомогою проводів а також без участі транзисторів. Тому бітові перестановки є дуже ефективним компонентом. Слід зазначити, що також можливі більш складні методи розсіювання, такі як рівень перемішування стовпців, який використовують в AES [18]. Незважаючи на те, що вони мають

криптографічні переваги, вони потребують більш високу вартість обладнання.

Захищеність шифру сильно залежить від криптографічних властивостей S-блоків. Наприклад, шифр AES [18] використовує 8-бітові S-блоки, що базуються на знаходженні оберненого (інверсії) в кінцевому полі з 2^8 елементів. Цей S-блок має найменшу відому диференціальну ймовірність та лінійну кореляцію, що позволяє AES бути захищеним з невеликою кількістю циклів, та досягати високої продуктивності. Тим не менш, це не завжди найкращий варіант для обмежених умов.

Багато блокових шифрів, та деякі потокові шифри, використовують S-блоки, щоб ввести нелінійність. У програмному забезпеченні S-блоки часто реалізуються як «look-up» таблиці (LUT). В апаратних засобах ці таблиці можуть мати більшу площу, або вони можуть створювати технологічні проблеми, так як поєднання комбінаторної логіки і захищених сегментів не завжди може легко досягатися за допомогою стандартного потоку конструкції апаратних засобів. Тому чисто комбінаторна реалізація часто є більш ефективною.

Якщо комбінаторні реалізації не використовують будь-якої внутрішньої структури в S-блоках, то вимоги до площі будуть швидко рости з числом вхідних і вихідних бітів. Чим більше вихідних бітів S-блок має, тим більше необхідно булевих рівнянь. І чим більше вхідних бітів має S-блок, тим складніші ці рівняння будуть. Можна спостерігати цікаву взаємодію між криптографією і апаратною реалізацією: для того, щоб витримувати диференціальний [3] та лінійний [4] криптоаналіз, висока нелінійність S-блоків не потрібна. В свою чергу вона безпосередньо впливає на високу кількість гейтів.

Галузь легковагової криптографії створює багато альтернатив з меншою площею. Зокрема, багато легковагових шифрів використовують S-блоки, що працюють на чотирьохбітних словах, або навіть на меншому алфавіті. Однак, скорочення числа змінних збільшує значення оптимальної диференціальної ймовірності та лінійної кореляції. Таким

чином, збільшення циклів потрібні для того, щоб досягти стійкість до диференціальних та лінійних атак.

Альтернативний підхід при побудові легковагового шифру полягає у використанні великих S-блоків, зазвичай працюючих на восьми бітах, так само як AES [18], але з більш низькою вартістю реалізації. Тоді, необхідно знайти S-блоки з кращою реалізацією ніж S-блоки у AES, за рахунок неоптимальних криптографічних властивостей. Знаходження восьмибітних S-блоків, які пропонують такий цікавий компроміс, це дуже важка проблема: вони не можуть бути класифіковані як у випадку чотирьохбітних, і випадково обрані S-блоки мають високу вартість реалізації. Тому необхідно орієнтуватися на конструкції, що основані на менших S-блоках та лінійних операціях. Цей підхід вже був використаний в декількох конструкціях, а саме: Crypton v0.5 [19], Crypton v1.0 [20], Whirlpool [21], Khazad [22], Iceberg [23], Zorro [24] та LS-Designs [25]. Вже визначено, що тираундова схема Фейстеля або тираундова схема MISTY мають такі криптографічні властивості, тому що вони використовують лише три невеликих S-блока, але можуть забезпечувати хороші великі S-блоки.

Схеми Фейстеля та MISTY інтенсивно вивчалися в контексті проектування блокових шифрів, тому відомі оцінки для максимальної середньої ймовірності диференціалу та максимального середнього лінійного потенціалу (MEDP, MELP). Однак ці результати не мають значення для побудови S-блоків, тому що вони враховують лише середнє значення по всіх ключах, тоді як S-блоки – безключові. Таким чином, диференціальні та лінійні властивості схеми Фейстеля та MISTY були проаналізовані у безключовому випадку.

Таке дослідження було розпочато нещодавно Лі та Вангом у випадку трьох циклів схеми Фейстеля. У роботі [1] Лі та Ванг одержали аналітичні оцінки для диференціальних імовірностей та лінійних потенціалів для тираундової безключової схеми Фейстеля; ці оцінки побудовані на основі значень диференціальних імовірностей та лінійних

потенціалів раундових перетворень (S-блоків) схеми Фейстеля. А.Канто та ін. [2] покращили ці оцінки та поширили їх на трираундову схему MISTY. У бакалаврській дипломній роботі було одержано аналітичні оцінки для диференціальних імовірностей та лінійних потенціалів для трираундової безключової R-схеми. [31]

1.2.2 Побудова S-блоків з блоків меншого розміру

Якщо в цій роботі ми зосередимося на побудові S-Box, використовуючи кілька менших S-Box. Дійсно, маленькі S-Box є набагато дешевше для реалізації великих S-Box:

– для реалізації програм на основі таблиці, розмір таблиці меньший;

– для апаратних реалізацій кількість графів менше;

– для реалізації програмного забезпечення з розрізом бітів, кількість команд нижче;

– для векторної реалізації малі S-блоки можуть використовувати векторні перестановки.

У багатьох випадках реалізація декількох невеликих S-блоків потребує менших ресурсів, ніж реалізація великих S-блоків. Таким чином, побудова S-блоку з менших може зменшити вартість впровадження.

Схема Фейстеля є відомою для побудови 2n-бітової перестановки з менших n-бітних функцій, введених у 1971 році для проектування Люцифера (який пізніше став DES). Це хороший кандидат для побудови великих S-блоків з менших за розумною ціною впровадження. Зокрема, ця конструкція використана для S-блоків Crypton v0.5, ZUC (для S0), Robin та iScream. Конструкція MISTY, введена Мацуї, використовує іншу структуру, але пропонує схожий рівень безпеки. Головною перевагою мережі MISTY є те, що він може запропонувати зменшену затримку,

оскільки перші два S-блоки можуть бути оцінені паралельно. Тому вона є природною альтернативою схемам Фейстеля для побудови легких S-блоків, і вона була використана при проектуванні Fantomas і Scream. Для того, щоб зменшити кількість воріт, що використовуються для реалізації конструкції, ми зосередимося на збалансованих схемах CLEFIA. [2]

1.3 Необхідні терміни та позначення

1.3.1 Узагальнена схема Фейстеля

Схема Фейстеля є однією з найбільш часто використовуваних структур в ітераційних блокових шифрах. [32]

Фундаментальним будівельним блоком схеми Фейстеля є F-функція: ключове залежне відображення вхідного рядка на вихідний рядок. F-функція завжди нелінійна і майже завжди незворотна.

Визначення 1.1. F-функція збалансованної схеми Фейстеля може бути виражена як:

$$F : \{0,1\}^{n/2} \times \{0,1\}^{k} \rightarrow \{0,1\}^{n/2}.$$

У цьому визначенні n є розмір блоку, n - парне. F є функцією, яка приймає $n/2$ бітів і k бітів ключа в якості вхідного сигналу, і виробляє вихід довжиною $n/2$ бітів.

Визначення 1.2. Одним раундом збалансованної мережі Фейстеля є:

$$X_{i+1} = (F_{k_i}(msb_{n/2}(X_i)) \oplus lsb_{n/2}(X_i))||msb_{n/2}(X_i)$$

Тут X_i є входом до раунду, X_{i+1} є виходом раунду, k_i є ключем, n - довжиною блоку, $lsb_u(x)$ і $msb_u(x)$ вибирають найменш значущі і

найбільш значущі біти x відповідно, mod вказує додавання по модулю 2, і $||$ вказує конкатенацію. У кожному раунді діє $msb_{n/2}(X_i)$ за допомогою ключової залежної нелінійної F-функції на $lsb_{n/2}(X_i)$. Це часто називають «лівою половиною», що діє на «правій половині».

Визначення 1.3. Збалансована схема Фейстеля складається з j раундів, де:

$$X_{i+1} = (F_{k_i}(msb_{n/2}(X_i)) \oplus lsb_{n/2}(X_i))||msb_{n/2}(X_i)$$

Ключі k_i є раундовими ключами, які зазвичай виводяться з алгоритму розкладу ключа на вхід ключа K. [33]

Структура Фейстеля забезпечує обернені перетворення незалежно від того, чи раундова функція F обратна або ні, і може бути використана для генерації випадкових перестановок від випадкових функцій.

Однією з корисних функцій класичної схеми Фейстеля є те, що вона забезпечує розсіювання вхідних блоків. Після двох раундів мережі розсіювання завершено, тобто обидва вихідних блоку залежать від обох вхідних блоків. Однак для сильного шифру цього недостатньо. Крім того, необхідно вимагати, щоб раундова функція мала гарні властивості розсіювання та перемішування. Схема Фейстеля використовується для поширення цих властивостей по всьому блоку шифру. Можуть бути ідентифіковані три підходи до проектування раундової функції.

Перший підхід, який використовується в DES, полягає в тому, щоб побудувати раундову функцію з набору паралельних перетворень заміни, S-блоків, і «склеювати» S-блоки разом, розширюючи вхідні дані так, щоб два сусідні S-блоки ділилися деяким входом, а також шляхом перестановки вихідних бітів набору S-блоків. Ця перестановка має суттєвий вплив на криптографічні властивості схеми і являє собою складний проектний виклик у відсутності теоретичної підтримки.

Другий підхід полягає у використанні тільки одного великого захищеного S-блоку. Така мережа Фейстеля є безумовно стійкою до

певних диференційних і лінійних криптоаналітичних атак. У теоретичних прикладах таких схем раундові функції були простими алгебраїчними функціями, які можуть викликати інші слабкості. Нещодавно М. Мацуї запропонував нову структуру шифру схеми Фейстеля, де раундова функція сама по собі є схемою Фейстеля. Ця схема виявилася захищеною від диференційного та лінійного криптоаналізу, що може бути показано шляхом повторення існуючих результатів безпеки для структур Фейстеля. Таким чином, починаючи з малих S-блоків, можна на кожній ітерації подвоїти розмір S-блоку, щоб отримати достатньо великі і міцні S-блоки.

По-третє, було запропоновано використовувати саму схему для отримання достатнього розсіювання. Цей підхід був використаний при проектуванні геш-функцій MD4, MD5 і HAVAL, які є прикладами того, що називаються загалом незбалансованими мережами Фейстеля. У більшості випадків блоки введення даних X_1 і X_2 мають різні розміри і, отже, входи і виходи раундової функції мають різну довжину.

Мета цього внеску полягає в тому, щоб показати, що перевірена безпека від диференціалу та лінійного криптоаналізу може бути досягнута за допомогою мережі малих S-блоків. Основними перевагами невеликих S-блоків є те, що вони можуть бути реалізовані у вигляді таблиць, і якщо вони генеруються випадковим чином, вони можуть бути ефективно перевірені на необхідні властивості.

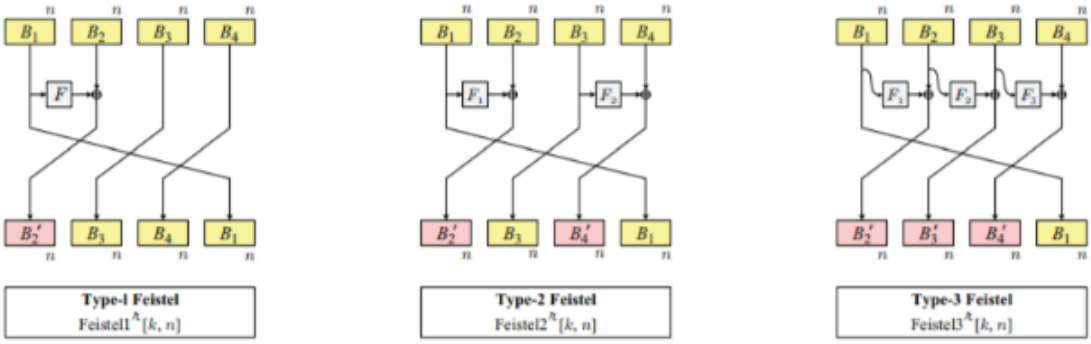

Рисунок 1.2 – Типи узагальненої схеми Фейстеля [32].

В данній роботі використовується другий підхід і досліджується ітераційна структура, яка називається узагальненою схемою Фейстеля. Раундова функція цієї мережі слабка в порівнянні з іншими. Вона складається тільки з набору паралельних S-блоків з однаковими вхідними та вихідними розмірами. Схема збалансована, тобто вхідні блоки X_1 і X_2 мають однакову довжину, але замість заміни двох вихідних блоків ми розділяємо вихідні блоки на підблоки, які потім переставляються. Таким чином,S-блок поступово поширюється за допомогою схеми, без допоміжних перестановок в раундовій функції. [32]

1.3.2 Диференціальний криптоаналіз

Як відомо, диференційний криптоаналіз є атакою обраного тексту, в якій статистична ключова інформація виводиться з блоків зашифрованого тексту, отриманих шляхом шифрування пар блоків відкритого тексту з певною побітовою різницею під цільовим ключем. Досліджено поширення вхідних різниць до різниць у вихідних перетвореннях.

Нехай $f : GF(2)^m \longmapsto GF(2)^m$ - булеве відображення, що складається з декількох раундів. Була введена концепція характеристик: послідовність різницевих моделей така, що вихідна різниця від одного раунду відповідає вхідній різниці в наступному раунді. З іншого боку була представлена концепція диференціала, позначена $\alpha \xrightarrow{f} \beta$, де XOR в входах і виходах проміжних раундів не фіксовані. Позначимо $DP(\alpha \xrightarrow{f} \beta) = Pr(f(x) + f(x + \alpha) = \beta)$, де α, β є фіксованими вхідними та вихідними різницями.

Диференціальний криптоаналіз використовує диференціальні характеристики з високою ймовірністю. Однак, навіть якщо максимальна диференційна характеристична ймовірність низька, не можна зробити

висновок, що шифр захищений від диференціального нападу. Натомість треба показати, що максимальна диференційна ймовірність всіх диференціалів є досить низькою. Ця властивість забезпечує доказову захищеність від диференціального криптоаналізу, на відміну від практичної безпеки, яка просто враховує ймовірність максимальної диференціальної характеристики.

Теорема 1.1. *Блоковий шифр з довжиною блоку m стійкий проти звичайних диференційних нападів при незалежному ключовому припущені, якщо не існує будь-якого диференціального $\alpha \to \beta$, $\alpha \neq 0$, що варіюється на всі, крім кількох раундів, таке що $DP(\alpha \to \beta) >> 2^{-m}$ [34].*

У роботі розглядаються S-блоки, що мають однакову кількість вхідних та вихідних бітів. Стійкість до диференціального та лінійного криптоаналізу визначається максимальним значенням у таблиці розподілів диференціалів (таблиці лінійних апроксимацій відповідно) [5]. Визначимо ці параметри формально.

Нехай V_n – множина всіх n-бітових векторів і F – це відображення з V_n на V_n. Для будь-якої пари різниць (a,b) з V_n^2 визначимо множину

$$D_F(a \to b) = \{x \in F_n^2 \mid F(x \oplus a) \oplus F(x) = b\}.$$

Комірка з індексом (a,b) в таблиці розподілів диференціалів F тоді відповідає потужності множини $D_F(a \to b)$; позначимо її як $\delta_F(a,b)$.

Диференціальна рівномірність F – це величина

$$\delta(F) = \max_{a \neq 0, b} \delta_F(a,b)$$

Максимальна імовірність диференціалу MDP пов'язана із диференціальною рівномірністю очевидним чином: $MDP(F) = \delta(F)/2^n$. Для будь-яких перетворень F справедлива оцінка $\delta(F) \geq 2$. Функції F, для яких виконується рівність, називаються майже досконалими нелінійними функціями (almost perfect nonlinear mappings, APN).[6]

1.3.3 Лінійний криптоаналіз

Лінійний криптоаналіз – це атака з відомим відкритим текстом, який намагається використати випадки лінійних виразів з високою ймовірністю, що включають біти відкритого тексту, біти шифрувального тексту та біти раундових ключів.

Як і в випадку з диференціалами ми також повинні розрізняти лінійну характеристику і лінійну оболонку. Лінійна характеристика над f складається з послідовності значень маски, так що значення вихідної маски від одного раунду відповідає значенням вхідної маски для наступного раунду. З іншого боку, лінійна оболонка, позначена $u \overset{f}{\leftarrow} w$, є сукупністю всіх лінійних характеристик з однаковими початковими та кінцевими значеннями маски. Позначимо $LP(u \overset{f}{\leftarrow} w) = [2 \cdot Pr(u \cdot f(x) = w \cdot x) - 1]^2$, де w, u є фіксованими значеннями вхідних і вихідних масок.

Лінійний криптоаналіз використовує переваги лінійних характеристик з високою ймовірністю кореляції для відновлення бітів ключа. Проте, при оцінці міцності блокового шифру проти лінійного криптоаналізу, слід розглянути лінійні оболонки. Маючи низьку лінійну ймовірність оболонки для всіх лінійних оболонок, це гарантує доказову безпеку від лінійних атак.

Теорема 1.2. *Блоковий шифр з довжиною блоку m стійкий проти звичайного лінійного криптоаналізу при незалежному ключовому припущені, якщо не існує лінійна оболонка $u \leftarrow w$, $u \neq 0$, що варіюється за всіма, крім декількох раундів, таке, що $LP(u \leftarrow w) >> 2^m$ [34].*

Перетворення Уолша відображення F – це функція

$$\lambda : V_n^2 \times V_n^2 \to Z$$
$$(a,b) \longmapsto \lambda_F(a,b) = \sum_{x \in V} (-1)^{b \cdot F(x) \oplus a \cdot x}$$

де крапкою позначено скалярний добуток бітових векторів.

Нелінійність F – це величина

$$\mathcal{L}(F) = \max_{a,b \in V_n^2, b \neq 0} |\lambda_F(a,b)|$$

Дійсно, з точністю до множника 2^n нелінійність відповідає імовірності неспівпадіння значення функції F та її найкращої лінійної апроксимації:

$$Pr_X[b \cdot F(x) + a \cdot X = 1] = \frac{1}{2^n}(2^{n-1} - \frac{1}{2} \sum_{x \in F_n^2} (-1)^{b \cdot F(x) \oplus a \cdot x}) = \frac{1}{2}(1 - \frac{\lambda_F(a,b)}{2^n})$$

Варто зауважити, що для будь-якої фіксованої вихідної маски $b \in V_n$ функція $a \longmapsto \lambda_F(a,b)$ відповідає перетворенню Уолша n-змінної булевої функції $b \cdot F(x)$, що є лінійною комбінацією координатних функцій F.

1.3.4 CLEFIA

CLEFIA являє собою 128-бітовий блоковий шифр з довжиною ключів 128, 192 і 256 біт, що сумісно з інтерфейсом AES. Алгоритм CLEFIA був опублікований в 2007 році, і його безпека була ретельно досліджена в громадській спільноті. CLEFIA є одним з нових поколінь легких блокових алгоритмів, розроблених після AES. Серед них, CLEFIA пропонує високу продуктивність програмного та апаратного забезпечення, а також легку реалізацію апаратних засобів. CLEFIA буде корисний для Інтернету, який буде підключений до більш розподілених і обмежених пристроїв.

CLEFIA – це 2n-бітовою блоковою схемою з узагальненою структурою Фейстеля. Специфікація блокового шифру CLEFIA визначає три довжини ключа: 128, 192 і 256 біт. Схема CLEFIA наведена на рисунку 3. Вхід має 16 байтів P0 - P15, згрупованих у чотири 4 байтові слова. Є 18 раундів і в кожному раунді перше і третє слова подаються в нелінійні функції F0 і F1 відповідно. Вихідні дані F0 і F1, загальновідомі як функції F, виходять з другого і четвертого слів. Крім того, друге і четверте слово також відбілюються на початку і в кінці шифрування. Нелінійність у F-функціях створюється двома S-блоками $S0$ та $S1$. Ці S-блоки мають вигляд таблиць з 256 байт, і викликаються двічі в кожній функції F, що робить загалом вісім табличних переглядів на раунд і 144 ($= 8 * 18$) переглядів на кодування. Рівняння для функцій $F0$ і $F1$ показані далі:

$$F_0 : (y_0,y_1,y_2,y_3) = (z_0,z_1,z_2,z_3) \cdot M0;$$
$$F_1 : (y_0,y_1,y_2,y_3) = (z'_0,z'_1,z'_2,z'_3) \cdot M1.$$

де

$$z_0 = S0[x_0 \oplus k_0] \qquad z_1 = S1[x_1 \oplus k_1]$$
$$z_2 = S0[x_2 \oplus k_2] \qquad z_3 = S1[x_2 \oplus k_2]$$

та

$$z'_0 = S1[x_0 \oplus k_0] \qquad z'_1 = S0[x_1 \oplus k_1]$$
$$z'_2 = S1[x_2 \oplus k_2] \qquad z'_3 = S0[x_2 \oplus k_2]$$

Функції F приймають 4 вхідних байти, x_0, x_1, x_2, x_3 і 4 раундові ключі, k_0, k_1, k_2 і k_3. Після look-ups S-блока, байти перемішуються, помноживши їх на (4×4) матриці $M0$ і $M1$ відповідно. Матриці $M0$ і $M1$ визначаються

наступним чином [35]:

$$M0 = \begin{pmatrix} 1 & 2 & 4 & 6 \\ 2 & 1 & 6 & 4 \\ 4 & 6 & 1 & 2 \\ 6 & 4 & 2 & 1 \end{pmatrix}, \qquad M1 = \begin{pmatrix} 1 & 8 & 2 & A \\ 8 & 1 & A & 2 \\ 2 & A & 1 & 8 \\ A & 2 & 8 & 1 \end{pmatrix},$$

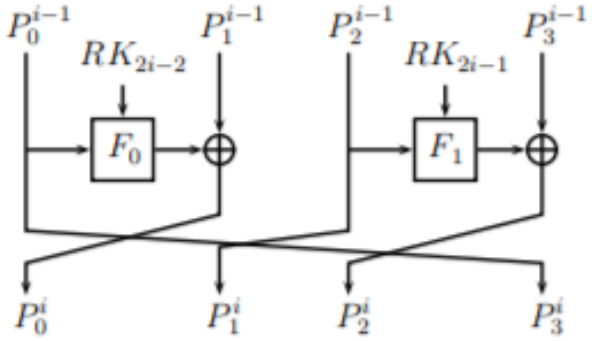

Рисунок 1.3 – Один раунд схеми CLEFIA

Алгоритм шифрування. Позначимо через $P = P_0|P_1|P_2|P_3$ 128-бітний відкритий текст, де кожен P_i, $i = 0, 1, 2, 3$, є 32-розрядним вектором. Позначимо через C відповідний зашифрований текст. CLEFIA підтримує ключі розміром 128, 192 або 256 біт, а загальна кількість ітерацій, нехай буде R, залежить від розміру ключа. Точніше, $R = 18$ для 128-бітової версії, тоді як $R = 22$ і $R = 26$ для двох наступних варіантів. Алгоритм генерації ключів, опис якого опускається, оскільки надалі розглядатиметься безключова версія схеми CLEFIA, використовується для генерації $2R$ раундових ключів RK_0,. . . , RK_{2R-1} та 4 ключі відбілювання WK_0,..., WK_3.

Шифрування виконується наступним чином:

– $P_0^0|P_1^0|P_2^0|P_3^0 = P_0|P_1 \oplus WK_0|P_2|P_3 \oplus WK_1$

– Для $i = 1, 2, ..., R$ виконати:
  – $P_0^i = F_0(P_0^{i-1}, RK_{2i-2}) \oplus P_1^{i-1}$
  – $P_1^i = P_2^{i-1}$
  – $P_2^i = F_1(P_2^{i-1}, RK_{2i-1}) \oplus P_3^{i-1}$
  – $P_3^i = P_0^{i-1}$
– $C = P_0^R | P_1^R \oplus WK_2 | P_2^R | P_3^R \oplus WK_3$.

Раундові функції F_0, F_1. Кожен раунд CLEFIA складається з двох 32-бітних круглих функцій F_0 і F_1 (див. Малюнок 3), які мають однакову структуру. Першим кроком у функції F_0 (відповідно F_1) є XOR між 32-бітним підключем RK_{2i-2} (відповідно, RK_{2i-1}) і P_0^{i-1} (відповідно P_2^{i-1}). Потім два 8×8-бітові S-блоки $S0$ і $S1$ складають рівень, який застосовується до результату. Нарешті, чотири отриманих байта змішуються 4×4-байтовою матрицею, $M0$ (відповідно $M1$), що має максимальний номер відгалуження, тобто 5. Детальний опис S-блоків $S0$, $S1$, а також матриць $M0$, $M1$ можна знайти в [36].

1.3.5 Аналіз структур криптографічних блокових перетворень за допомогою фіксованого ключа

Для вивчення властивостей схем ітеративного криптографічних блокових перетворень для побудови легковагових S-блоків, необхідно вивчити ці структури з фіксованим ключем. Аналогічно, можна розглянути структури без будь-якого ключа, так як структура з фіксованим ключем еквівалентна безключевій з різними S-блоками. Дійсно, використання S-блоків S_i з раундовим ключем k_i еквівалентно використанню $S_i' : x \to S_i(x + k_i)$ як S-блоку без ключа. Надалі завжди розглядається варіант з відсутнім ключем.

У аналізі структур Фейстеля з фіксованим ключем, Лі і Ванг [1]

витягти найкращу диференціальну однорідність і лінійність, які можуть бути досягнуті за допомогою трьохраундового перетворення Фейстеля з фіксованим ключем, і навели приклади досягнення цієї межі. Їх основні результати виглядають наступним чином:

Теорема 1.3. *Нехай S_1, S_2 та S_3 – це три n-бітні S-блоки та F – це 2n-бітна функція, визначена відповідною трьохраундовою схемою Фейстеля. Тоді $\delta(F) > 2\delta(S_2)$. Більш того, якщо S_2 не є перестановкою, тоді $\delta(F) > 2^{(n+1)}$.*

Якщо $n = 4$, F задовольняє $\delta(F) > 8$. Якщо має місце рівність, то $\mathcal{L}(F) > 64$.

Висновки до розділу 1

В даному розділі проаналізовано поняття легковагова криптографія та схеми безключового перетворення. Також отримано нові знання для подальшого дослідження даного напряму криптографії та виникли питання щодо стійкості даних систем проти диференціального та лінійного криптоаналізу. Іншими словами, виникла необхідність у виявленні диференціальних та лінійних властивостей схем безключових перетворень. Тобто необхідно оцінити сильно структуровані шифри через оцінки внутрішніх вузлів, з яких вони складаються.

2 ДИФЕРЕНЦІАЛЬНА РІВНОМІРНІСТЬ ТА НЕЛІНІЙНІСТЬ ДЛЯ CLEFIA

У даному розділі одержані оцінки диференціальної рівномірності та лінійного потенціалу для блокового безключового перетворення CLEFIA.

2.1 Диференціальна рівномірність для трираундової CLEFIA

Одержані оцінки диференціальної рівномірності для трираундової CLEFIA базуються на розгляданні окремих різниць, для яких вхідна різниця одного з раундових S-блоків дорівнює нулю.

Теорема 2.1. *Нехай S_1, S_2, S_3, S_4, S_5, та S_6 – це n-бітні S-блоки (не обов'язково різні), F – це $4n$-бітова функція, побудована за структурою трираундової CLEFIA із відображеннями S_1, S_2, S_3, S_4, S_5, та S_6 в якості раундових перетворень. Тоді для будь-яких a, b, c, d, p, k та m з F_2^n маємо:*

1) Якщо S_2 – бієктивний, то

$$\delta_F(0 \parallel 0 \parallel 0 \parallel a, a \parallel b \parallel c \parallel 0) = \delta_{S_4}(a, b) \times \delta_{S_6}(b, c);$$

2) Якщо S_4 – бієктивний, то

$$\delta_F(0 \parallel 0 \parallel a \parallel 0, d \parallel b \parallel c \parallel a) = \delta_{S_2}(a, z) \times \delta_{S_4}(z, b) \times \delta_{S_6}(b, c) \times \delta_{S_5}(a, d \oplus z);$$

3)

$$\delta_F(0 \parallel a \parallel 0 \parallel 0, c \parallel 0 \parallel a \parallel b) = \delta_{S_3}(a, b) \times \delta_{S_5}(b, c).$$

4) Якщо S_1 – бієктивний, то

$$\delta_F(a \parallel 0 \parallel 0 \parallel 0, c \parallel a \parallel d \parallel b) = \delta_{S_1}(a, z) \times \delta_{S_3}(z, b) \times \delta_{S_5}(b, c) \times \delta_{S_6}(a, d \oplus z);$$

5) Якщо S_3 – бієктивний, то

$$\delta_F(0 \parallel a \parallel b \parallel c, d \parallel k \parallel m \parallel 0) = \delta_{S_2}(b, c \oplus d) \times \delta_{S_4}(d, k) \times \delta_{S_6}(k, m \oplus a) \times \\ \times \delta_{S_3}(k, m \oplus a);$$

6)

$$\delta_F(c \parallel a \parallel 0 \parallel b, k \parallel 0 \parallel m \parallel p) = \delta_{S_1}(c, m \oplus a) \times \delta_{S_3}(m, p) \times \delta_{S_5}(k, k \oplus m) \times \\ \times \delta_{S_4}(b, c);$$

7) Якщо S_2 – бієктивний, то

$$\delta_F(c \parallel a \parallel b \parallel d, m \parallel 0 \parallel q \parallel p) = \delta_{S_1}(c, q \oplus a) \times \delta_{S_2}(b, z \oplus d) \times \delta_{S_3}(q, b \oplus p) \times \\ \times \delta_{S_5}(p, z \oplus m) \times \delta_{S_4}(z, c);$$

8)

$$\delta_F(0 \parallel a \parallel 0 \parallel b, m \parallel c \parallel k \parallel d) = \delta_{S_3}(a,d) \times \delta_{S_4}(b, c) \times \delta_{S_5}(d, b \oplus m) \times \\ \times \delta_{S_6}(c, k \oplus a);$$

9) Якщо S_1 – бієктивний, то

$$\delta_F(a \parallel b \parallel 0 \parallel 0, m \parallel a \parallel c \parallel d) = \delta_{S_1}(a,z) \times \delta_{S_3}(z, d) \times \delta_{S_5}(d, m) \times \delta_{S_6}(a,z \oplus c);$$

10) Якщо S_2 – бієктивний, то

$$\delta_F(0 \parallel 0 \parallel a \parallel b, m \parallel d \parallel c \parallel a) = \delta_{S_2}(a,z) \times \delta_{S_4}(z, d) \times \delta_{S_6}(d,c) \times \delta_{S_5}(a,z \oplus m).$$

Доведення.

Розглянемо випадки, для яких вхідна різниця одного з раундових

S-блоків дорівнює нулю:

Для S_1:
- $x \oplus (0||a||b||c)$
- $x \oplus (0||a||0||b)$
- $x \oplus (0||0||a||b)$
- $x \oplus (0||a||0||0)$
- $x \oplus (0||0||a||0)$

Для S_2:
- $x \oplus (a||b||0||c)$
- $x \oplus (a||b||0||0)$
- $x \oplus (0||a||0||b)$
- $x \oplus (0||0||0||a)$
- $x \oplus (0||a||0||0)$

Для S_3:
- $x \oplus (0||0||a||b)$
- $x \oplus (0||0||a||0)$
- $x \oplus (0||0||0||a)$
- $x \oplus (a||b||c||d)$, при
- $S_1(x_1) \oplus S_1(x_1 \oplus a) = b$

Для S_4:
- $x \oplus (a||b||0||0)$
- $x \oplus (a||0||0||0)$
- $x \oplus (0||a||0||0)$
- $x \oplus (c||d||a||b)$, при
- $S_2(x_3) \oplus S_2(x_3 \oplus a) = b$

Для S_5:
- $x \oplus (0||0||0||a)$, $S_1(x_1) \oplus S_1(x_1 \oplus a) = b$
- $x \oplus (a||b||0||c)$, $S_1(x_1) \oplus S_1(x_1 \oplus a) = b$
- $x \oplus (a||b||0||0)$, $S_1(x_1) \oplus S_1(x_1 \oplus a) = b$
- $x \oplus (c||d||a||b)$, $S_1(x_1) \oplus S_1(x_1 \oplus a) = b$ і $S_1(x_1) \oplus S_1(x_1 \oplus c) = d$

Для S_6:
- $x \oplus (0||a||0||0)$
- $x \oplus (c||d||a||b)$, $S_2(x_3) \oplus S_2(x_3 \oplus a) = b$

Якщо узагальнити усі випадки, отримаємо:

Випадок 1.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його чотири рівні частини. Розглянемо проходження різниці входів x та $x \oplus (0||0||0||a)$ через функцію F таким чином, щоб одержати на виході різницю $(a||b||c||0)$.

Перший раунд:

$$(x_2 \oplus S_1(x_1),x_3,x_4 \oplus S_2(x_3),x_1) \oplus (x_2 \oplus S_1(x_1),x_3,x_4 \oplus a \oplus S_2(x_3),x_1) = [0,0,a,0].$$

Другий раунд:

$$(S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_1(x_1) \oplus x_2) \oplus$$
$$\oplus (S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4 \oplus a, S_4(S_2(x_3) \oplus x_4 \oplus a) \oplus x_1, S_1(x_1) \oplus x_2) =$$
$$= [0, a, S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3) \oplus x_4 \oplus a, 0].$$

Третій раунд:

$$(S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1,$$
$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus$$
$$\oplus (S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4 \oplus a, S_4(S_2(x_3) \oplus x_4 \oplus a) \oplus x_1,$$
$$S_6(S_4(S_2(x_3) \oplus x_4 \oplus a) \oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3) = [a, b, c, 0].$$

Таким чином, вектор $x = (x_1, x_2, x_3, x_4)$ задовольняє

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F(x_1 \parallel x_2 \parallel x_3 \parallel (x_4 \oplus a)) = a \parallel b \parallel c \parallel 0$$

тоді і тільки тоді, коли:

$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_6(S_4(S_2(x_3) \oplus x_4 \oplus a) \oplus x_1) = c$$

$$S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3) \oplus x_4 \oplus a) = b$$

що рівносильно

$$x_4 \oplus S_2(x_3) \in D_{S_4}(a \to b)$$
$$x_1 \oplus S_4(S_2(x_3) \oplus x_4) \in D_{S_6}(b \to c),$$

якщо S_2 – бієктвний.

Таким чином доведено, що існує $\delta_{S_4}(a,b)$ значень x_4 та для кожного з них $\delta_{S_6}(b,c)$ значень x_1, таких що x досягає різниці.

Випадок 2.

Розглянемо проходження різниці входів x та $x \oplus (0||0||a||0)$ через

функцію F таким чином, щоб одержати на виході різницю $(d||b||c||a)$.

Перший раунд:

$$(x_2 \oplus S_1(x_1),x_3,x_4 \oplus S_2(x_3),x_1) \oplus (x_2 \oplus S_1(x_1),x_3 \oplus a,x_4 \oplus S_2(x_3 \oplus a),x_1) = \\ = [0,a,S_2(x_3) \oplus S_2(x_3 \oplus a),0].$$

Другий раунд:

$$(S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_1(x_1) \oplus x_2) \oplus \\ \oplus (S_3(x_2 \oplus S_1(x_1)) \oplus x_3 \oplus a, S_2(x_3 \oplus a) \oplus x_4, S_4(S_2(x_3 \oplus a) \oplus x_4) \oplus x_1, S_1(x_1) \oplus x_2) = \\ = [a, z, c, 0].$$

Третій раунд:

$$(S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, \\ S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus \\ \oplus (S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3 \oplus a) \oplus S_2(x_3 \oplus a) \oplus x_4, S_4(S_2(x_3 \oplus a) \oplus x_4) \oplus x_1, \\ S_6(S_4(S_2(x_3 \oplus a) \oplus x_4) \oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3 \oplus a) = \\ = [S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus S_5(S_3(S_1(x_1) \oplus x_2) \oplus \\ \oplus x_3 \oplus a) \oplus S_2(x_3 \oplus a), S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3 \oplus a) \oplus x_4), \\ S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_6(S_4(S_2(x_3 \oplus a) \oplus x_4) \oplus x_1), a].$$

Таким чином, вектор $x = (x_1, x_2, x_3, x_4)$ задовольняє

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F(x_1 \parallel x_2 \parallel (x_3 \oplus a) \parallel x_4) = d \parallel b \parallel c \parallel a$$

тоді і тільки тоді, коли:

$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_6(S_4(S_2(x_3 \oplus a) \oplus x_4) \oplus x_1) = c$$

$$S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3 \oplus a) \oplus x_4) = b$$

$$S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3 \oplus a) \oplus S_2(x_3 \oplus a) = d$$

$$S_2(x_3) \oplus S_2(x_3 \oplus a) = z$$

що рівносильно

$$x_3 \oplus S_3(S_1(x_1) \oplus x_2) \in D_{S_5}(a \to d \oplus z),$$

$$x_1 \oplus S_4(S_2(x_3) \oplus x_4) \in D_{S_6}(b \to c),$$

$$x_3 \in D_{S_2}(a \to z)$$

$$x_4 \oplus S_2(x_3) \in D_{S_4}(b \to c)$$

якщо S_4 – бієктвний.

Таким чином доведено, що для будь-якого фіксованого $z \in F_2^n$ таке, що існує $\delta_{S_5}(a \to d \oplus z)$ значень x_3, для кожного з яких існує $\delta_{S_4}(b,c)$ значень x_4 та для кожного з них $\delta_{S_6}(b,c)$ значень x_1, таких що x досягає різниці.

Випадок 3.

Розглянемо проходження різниці входів x та $x \oplus (0||a||0||0)$ через функцію F таким чином, щоб одержати на виході різницю $(c||0||a||b)$.

Перший раунд:

$$(x_2 \oplus S_1(x_1), x_3, x_4 \oplus S_2(x_3), x_1) \oplus (x_2 \oplus a \oplus S_1(x_1), x_3, x_4 \oplus S_2(x_3), x_1) = \\ = [a,0,0,0].$$

Другий раунд:

$$(S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_1(x_1) \oplus x_2) \oplus \\ \oplus (S_3(x_2 \oplus a \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_1(x_1) \oplus x_2 \oplus a) = \\ = [b,0,0,a].$$

Третій раунд:

$$(S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1,$$
$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus$$
$$\oplus (S_5(S_3(S_1(x_1) \oplus x_2 \oplus a) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1,$$
$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_1(x_1) \oplus x_2 \oplus a, S_3(S_1(x_1) \oplus x_2 \oplus a) \oplus x_3) =$$
$$= [c,0,a,b].$$

Таким чином, вектор $x = (x_1, x_2, x_3, x_4)$ задовольняє

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F(x_1 \parallel (x_2 \oplus a) \parallel x_3 \parallel x_4) = c \parallel 0 \parallel a \parallel b$$

тоді і тільки тоді, коли:

$$S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_5(S_3(S_1(x_1) \oplus x_2 \oplus a) \oplus x_3) = c$$

$$S_3(S_1(x_1) \oplus x_2) \oplus S_3(S_1(x_1) \oplus x_2 \oplus a) = b$$

що рівносильно

$$x_3 \oplus S_3(S_1(x_1) \oplus x_2) \in D_{S_5}(b \to c),$$

$$x_2 \oplus S_1(x_1) \in D_{S_3}(a \to b)$$

Таким чином доведено, що існує $\delta_{S_3}(a,b)$ значень x_2 та для кожного з них $\delta_{S_5}(b,c)$ значень x_1, таких що x досягає різниці.

Випадок 4.

Розглянемо проходження різниці входів x та $x \oplus (a||0||0||0)$ через функцію F таким чином, щоб одержати на виході різницю $(c||a||d||b)$.

Перший раунд:

$$(x_2 \oplus S_1(x_1),x_3,x_4 \oplus S_2(x_3),x_1) \oplus (x_2 \oplus S_1(x_1 \oplus a),x_3,x_4 \oplus S_2(x_3),x_1 \oplus a) =$$
$$= [S_1(x_1) \oplus S_1(x_1 \oplus a),0,0,a].$$

Другий раунд:

$$(S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_1(x_1) \oplus x_2) \oplus$$
$$\oplus (S_3(x_2 \oplus S_1(x_1 \oplus a)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1 \oplus a, S_1(x_1 \oplus a) \oplus x_2) =$$
$$= [S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus S_1(x_1 \oplus a)), 0, a, S_1(x_1) \oplus S_1(x_1 \oplus a)].$$

Третій раунд:

$$(S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1,$$
$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus$$
$$\oplus (S_5(S_3(S_1(x_1 \oplus a) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1 \oplus a,$$
$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1 \oplus a) \oplus S_1(x_1 \oplus a) \oplus x_2, S_3(S_1(x_1 \oplus a) \oplus x_2) \oplus x_3) =$$
$$= [S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_5(S_3(S_1(x_1 \oplus a) \oplus x_2) \oplus x_3), a,$$
$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_1(x_1) \oplus S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1 \oplus a) \oplus S_1(x_1 \oplus a),$$
$$S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus S_1(x_1 \oplus a))].$$

Таким чином, вектор $x = (x_1, x_2, x_3, x_4)$ задовольняє

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F((x_1 \oplus a) \parallel x_2 \parallel x_3 \parallel x_4) = c \parallel a \parallel d \parallel b$$

тоді і тільки тоді, коли:

$$S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_5(S_3(S_1(x_1 \oplus a) \oplus x_2) \oplus x_3) = c$$

$$S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus S_1(x_1 \oplus a)) = b$$

$$S_1(x_1) \oplus S_1(x_1 \oplus a) = z$$

$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_1(x_1) \oplus S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1 \oplus a) \oplus S_1(x_1 \oplus a) = d$$

що рівносильно

$$x_3 \oplus S_3(S_1(x_1) \oplus x_2) \in D_{S_5}(b \to c),$$

$$x_2 \oplus S_1(x_1) \in D_{S_3}(z \to b)$$

$$x_1 \in D_{S_1}(a \to z)$$

$$x_1 \oplus S_4(S_2(x_3) \oplus x_4) \in D_{S_6}(a \to d \oplus z)$$

якщо S_1 – бієктвний.

Таким чином доведено, що для будь-якого фіксованого $z \in F_2^n$ таке, що існує $\delta_{S_3}(z, b)$ значень x_2, для кожного з яких існує $\delta_{S_6}(a, d \oplus z)$ значень x_1 та для кожного з них $\delta_{S_5}(b,c)$ значень x_3, таких що x досягає різниці.

Випадок 5.

Розглянемо проходження різниці входів x та $x \oplus (0||a||b||c)$ через функцію F таким чином, щоб одержати на виході різницю $(d||k||m||0)$.

Перший раунд:

$$(x_2 \oplus S_1(x_1),x_3,x_4 \oplus S_2(x_3),x_1) \oplus (x_2 \oplus a \oplus S_1(x_1),x_3 \oplus b,x_4 \oplus c \oplus S_2(x_3 \oplus b),$$
$$x_1) = [a,b,S_2(x_3) \oplus S_2(x_3 \oplus b) \oplus c,0].$$

Другий раунд:

$$(S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_1(x_1) \oplus x_2) \oplus$$
$$\oplus (S_3(x_2 \oplus a \oplus S_1(x_1)) \oplus x_3 \oplus b, S_2(x_3 \oplus b) \oplus x_4 \oplus c, S_4(S_2(x_3 \oplus b) \oplus$$
$$\oplus x_4 \oplus c) \oplus x_1, S_1(x_1) \oplus x_2 \oplus a) = [S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus a \oplus$$
$$\oplus S_1(x_1)) \oplus b, S_2(x_3) \oplus S_2(x_3 \oplus b) \oplus c, S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3 \oplus b) \oplus x_4 \oplus c), a].$$

Третій раунд:

$$(S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1,$$
$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus$$
$$\oplus (S_5(S_3(S_1(x_1) \oplus x_2 \oplus a) \oplus x_3 \oplus b) \oplus S_2(x_3 \oplus b) \oplus x_4 \oplus c, S_4(S_2(x_3 \oplus b) \oplus x_4 \oplus c) \oplus x_1,$$
$$S_6(S_4(S_2(x_3 \oplus b) \oplus x_4 \oplus c) \oplus x_1) \oplus S_1(x_1) \oplus x_2 \oplus a, S_3(S_1(x_1) \oplus x_2 \oplus a) \oplus x_3 \oplus b) =$$

$$= [S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus S_2(x_3)\oplus S_5(S_3(S_1(x_1)\oplus x_2\oplus a)\oplus x_3\oplus b)\oplus S_2(x_3\oplus b)\oplus c,$$
$$S_4(S_2(x_3)\oplus x_4)\oplus S_4(S_2(x_3\oplus b)\oplus x_4\oplus c), S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)\oplus$$
$$\oplus S_6(S_4(S_2(x_3\oplus b)\oplus x_4\oplus c)\oplus x_1)\oplus a, S_3(x_2\oplus S_1(x_1))\oplus S_3(x_2\oplus a\oplus S_1(x_1))\oplus b].$$

Таким чином, вектор $x = (x_1, x_2, x_3, x_4)$ задовольняє

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F(x_1 \parallel (x_2 \oplus a) \parallel (x_3 \oplus b) \parallel (x_4 \oplus c)) = d \parallel k \parallel m \parallel 0$$

тоді і тільки тоді, коли:

$$S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus S_2(x_3)\oplus S_5(S_3(S_1(x_1)\oplus x_2\oplus a)\oplus x_3\oplus b)\oplus S_2(x_3\oplus b)\oplus c = d$$

$$S_4(S_2(x_3)\oplus x_4)\oplus S_4(S_2(x_3\oplus b)\oplus x_4\oplus c) = k$$

$$S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)\oplus S_6(S_4(S_2(x_3\oplus b)\oplus x_4\oplus c)\oplus x_1)\oplus a = m$$

$$S_3(x_2\oplus S_1(x_1))\oplus S_3(x_2\oplus a\oplus S_1(x_1))\oplus b = 0$$

що рівносильно

$$x_2 \oplus S_1(x_1) \in D_{S_3}(a \to b)$$

$$x_3 \in D_{S_2}(b \to c \oplus d)$$

$$x_4 \oplus S_2(x_3) \in D_{S_4}(d \to k)$$

$$x_1 \oplus S_4(S_2(x_3)\oplus x_4) \in D_{S_6}(k \to m \oplus a)$$

якщо S_3 – бієктвний.

Таким чином доведено, що існує $\delta_{S_2}(b, c\oplus d)$ значень x_3, для кожного з яких існує $\delta_{S_4}(d, k)$ значень x_4 та для кожного з них $\delta_{S_6}(k, m\oplus a)$ значень x_1 та для кожного з них $\delta_{S_3}(a, b)$ значень x_2, таких що x досягає різниці.

Випадок 6.

Розглянемо проходження різниці входів x та $x \oplus (c||a||0||b)$ через функцію F таким чином, щоб одержати на виході різницю $(k||0||m||p)$.

Перший раунд:

$$(x_2 \oplus S_1(x_1), x_3, x_4 \oplus S_2(x_3), x_1) \oplus (x_2 \oplus a \oplus S_1(x_1 \oplus c), x_3, x_4 \oplus c \oplus S_2(x_3),$$
$$x_1 \oplus c) = [a \oplus S_1(x_1) \oplus S_1(x_1 \oplus c), b, S_2(x_3) \oplus S_2(x_3) \oplus c, c].$$

Другий раунд:

$$(S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_1(x_1) \oplus x_2) \oplus$$
$$\oplus (S_3(x_2 \oplus a \oplus S_1(x_1 \oplus c)) \oplus x_3, S_2(x_3) \oplus x_4 \oplus c, S_4(S_2(x_3) \oplus x_4 \oplus c) \oplus x_1 \oplus c,$$
$$S_1(x_1 \oplus c) \oplus x_2 \oplus a) = [S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus a \oplus S_1(x_1 \oplus c)) \oplus b, S_2(x_3) \oplus S_2 \oplus c,$$
$$S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3) \oplus x_4 \oplus c) \oplus c, a \oplus S_1(x_1) \oplus S_1(x_1 \oplus c)].$$

Третій раунд:

$$(S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_6(S_4(S_2(x_3) \oplus x_4) \oplus$$
$$\oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus (S_5(S_3(S_1(x_1 \oplus c) \oplus x_2 \oplus a) \oplus x_3) \oplus$$
$$\oplus S_2(x_3) \oplus x_4 \oplus c, S_4(S_2(x_3) \oplus x_4 \oplus c) \oplus x_1 \oplus c, S_6(S_4(S_2(x_3) \oplus x_4 \oplus c) \oplus$$
$$\oplus x_1 \oplus c) \oplus S_1(x_1 \oplus c) \oplus x_2 \oplus a, S_3(S_1(x_1 \oplus c) \oplus x_2 \oplus a) \oplus x_3) = [S_5(S_3(S_1(x_1) \oplus x_2) \oplus$$
$$\oplus x_3) \oplus S_2(x_3) \oplus S_5(S_3(S_1(x_1 \oplus c) \oplus x_2 \oplus a) \oplus x_3) \oplus S_2(x_3) \oplus c, S_4(S_2(x_3) \oplus x_4) \oplus$$
$$\oplus S_4(S_2(x_3) \oplus x_4 \oplus c) \oplus c, S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_6(S_4(S_2(x_3) \oplus x_4 \oplus c) \oplus$$
$$\oplus x_1 \oplus c) \oplus S_1(x_1) \oplus S_1(x_1 \oplus c) \oplus a, S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus a \oplus S_1(x_1 \oplus c)) \oplus b].$$

Таким чином, вектор $x = (x_1, x_2, x_3, x_4)$ задовольняє

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F((x_1 \oplus c) \parallel (x_2 \oplus a) \parallel x_3 \parallel (x_4 \oplus b)) = k \parallel 0 \parallel m \parallel p$$

тоді і тільки тоді, коли:

$$S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus S_5(S_3(S_1(x_1 \oplus c) \oplus x_2 \oplus a) \oplus x_3) \oplus S_2(x_3) \oplus c = k$$

$$S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3) \oplus x_4 \oplus c) \oplus c = 0$$

$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_6(S_4(S_2(x_3) \oplus x_4 \oplus c) \oplus x_1 \oplus c) \oplus S_1(x_1) \oplus S_1(x_1 \oplus c) \oplus a = m$$

$$S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus a \oplus S_1(x_1 \oplus c)) \oplus b = p$$

що рівносильно

$$x_2 \oplus S_1(x_1) \in D_{S_3}(m \to p)$$

$$x_4 \oplus S_2(x_3) \in D_{S_4}(b \to c)$$

$$x_3 \oplus S_3(S_1(x_1) \oplus x_2) \in D_{S_5}(p \to k \oplus b)$$

$$x_1 \in D_{S_1}(c \to m \oplus a)$$

Таким чином доведено, що існує $_{S_1}(c, m \oplus a)$ значень x_1, для кожного з яких існує $\delta_{S_3}(m, p)$ значень x_2 та для кожного з них $\delta_{S_5}(p, k \oplus b)$ значень x_3 та для кожного з них $\delta_{S_4}(b, c)$ значень x_4, таких що x досягає різниці.

Випадок 7.

Розглянемо проходження різниці входів x та $x \oplus (c||a||b||d)$ через функцію F таким чином, щоб одержати на виході різницю $(m||0||q||p)$.

Перший раунд:

$$(x_2 \oplus S_1(x_1),x_3,x_4 \oplus d \oplus S_2(x_3),x_1) \oplus (x_2 \oplus a \oplus S_1(x_1 \oplus c),x_3 \oplus b,x_4 \oplus d \oplus$$
$$\oplus S_2(x_3 \oplus b), x_1 \oplus c) = [a \oplus S_1(x_1) \oplus S_1(x_1 \oplus c),b,S_2(x_3) \oplus S_2(x_3 \oplus b),c].$$

Другий раунд:

$$(S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4 \oplus d, S_4(S_2(x_3) \oplus x_4 \oplus d) \oplus x_1, S_1(x_1) \oplus x_2) \oplus$$
$$\oplus (S_3(x_2 \oplus a \oplus S_1(x_1 \oplus c)) \oplus x_3 \oplus b, S_2(x_3 \oplus b) \oplus x_4 \oplus d, S_4(S_2(x_3 \oplus b) \oplus x_4 \oplus d) \oplus x_1 \oplus c,$$
$$S_1(x_1 \oplus c) \oplus x_2 \oplus a) = [S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus a \oplus S_1(x_1 \oplus c)) \oplus b, S_2(x_3) \oplus S_2(x_3 \oplus b),$$
$$S_4(S_2(x_3) \oplus x_4 \oplus d) \oplus S_4(S_2(x_3 \oplus b) \oplus x_4 \oplus d) \oplus c, a \oplus S_1(x_1) \oplus S_1(x_1 \oplus c)].$$

Третій раунд:

$$(S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4 \oplus d, S_4(S_2(x_3) \oplus x_4 \oplus d) \oplus x_1,$$

$$S_6(S_4(S_2(x_3)\oplus x_4\oplus d)\oplus x_1)\oplus S_1(x_1)\oplus x_2, S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus$$
$$\oplus(S_5(S_3(S_1(x_1\oplus c)\oplus x_2\oplus a)\oplus x_3\oplus b)\oplus S_2(x_3\oplus b)\oplus x_4\oplus d, S_4(S_2(x_3\oplus b)\oplus x_4\oplus d)\oplus x_1\oplus$$
$$\oplus c, S_6(S_4(S_2(x_3\oplus b)\oplus x_4\oplus d)\oplus x_1\oplus c)\oplus S_1(x_1\oplus c)\oplus x_2\oplus a, S_3(S_1(x_1\oplus c)\oplus x_2\oplus a)\oplus$$
$$\oplus x_3\oplus b) = [S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus S_2(x_3)\oplus S_5(S_3(S_1(x_1\oplus c)\oplus x_2\oplus a)\oplus x_3\oplus b)\oplus$$
$$\oplus S_2(x_3\oplus b), S_4(S_2(x_3)\oplus x_4\oplus d)\oplus S_4(S_2(x_3\oplus b)\oplus x_4\oplus d)\oplus c, S_6(S_4(S_2(x_3)\oplus x_4\oplus d)\oplus$$
$$\oplus x_1)\oplus S_6(S_4(S_2(x_3\oplus b)\oplus x_4\oplus d)\oplus x_1\oplus c)\oplus S_1(x_1)\oplus S_1(x_1\oplus c)\oplus a, S_3(x_2\oplus S_1(x_1))\oplus$$
$$\oplus S_3(x_2\oplus a\oplus S_1(x_1\oplus c))\oplus b].$$

Таким чином, вектор $x = (x_1, x_2, x_3, x_4)$ задовольняє

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F((x_1 \oplus c) \parallel (x_2 \oplus a) \parallel (x_3 \oplus b) \parallel (x_4 \oplus d)) =$$
$$= m \parallel 0 \parallel q \parallel p$$

тоді і тільки тоді, коли:

$$S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus S_2(x_3)\oplus S_5(S_3(S_1(x_1\oplus c)\oplus x_2\oplus a)\oplus x_3\oplus b)\oplus S_2(x_3\oplus b = m$$

$$S_4(S_2(x_3)\oplus x_4\oplus d)\oplus S_4(S_2(x_3\oplus b)\oplus x_4\oplus d)\oplus c = 0$$

$$S_6(S_4(S_2(x_3)\oplus x_4\oplus d)\oplus x_1)\oplus S_6(S_4(S_2(x_3\oplus b)\oplus x_4\oplus d)\oplus x_1\oplus c)\oplus$$
$$\oplus S_1(x_1)\oplus S_1(x_1\oplus c)\oplus a = q$$

$$S_3(x_2\oplus S_1(x_1))\oplus S_3(x_2\oplus a\oplus S_1(x_1\oplus c))\oplus b = p$$

що рівносильно

$$x_2 \oplus S_1(x_1) \in D_{S_3}(q \to b \oplus p)$$

$$x_3 \in D_{S_2}(b \to z \oplus d)$$

$$x_4 \oplus d \oplus S_2(x_3) \in D_{S_4}(z \to c)$$

$$x_3 \oplus S_3(S_1(x_1) \oplus x_2) \in D_{S_5}(p \to z \oplus m)$$

$$x_1 \in D_{S_1}(c \to q \oplus a)$$

якщо S_2 – бієктвний.

Таким чином доведено, що для будь-якого фіксованого $z \in F_2^n$ таке, що існує $\delta_{S_2}(b, z \oplus d)$ значень x_3, для кожного з яких існує $\delta_{S_4}(z, c)$ значень x_4 та для кожного з них $\delta_{S_1}(c, q \oplus a)$ значень x_1 та для кожного з них $\delta_{S_3}(q, b \oplus p)$ значень x_2, таких що x досягає різниці.

Випадок 8.

Розглянемо проходження різниці входів x та $x \oplus (0||a||0||b)$ через функцію F таким чином, щоб одержати на виході різницю $(m||c||k||d)$.

Перший раунд:

$$(x_2 \oplus S_1(x_1),x_3,x_4 \oplus b \oplus S_2(x_3),x_1) \oplus (x_2 \oplus a \oplus S_1(x_1),x_3,x_4 \oplus b \oplus S_2(x_3),$$
$$x_1) = [a \oplus S_1(x_1) \oplus S_1(x_1),b,S_2(x_3) \oplus S_2(x_3),c].$$

Другий раунд:

$$(S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4 \oplus b, S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus x_1, S_1(x_1) \oplus x_2) \oplus$$
$$\oplus (S_3(x_2 \oplus a \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4 \oplus b, S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus x_1,$$
$$S_1(x_1) \oplus x_2 \oplus a) = [S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus a \oplus S_1(x_1)), S_2(x_3) \oplus S_2(x_3),$$
$$S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus S_4(S_2(x_3) \oplus x_4 \oplus b), a \oplus S_1(x_1) \oplus S_1(x_1)].$$

Третій раунд:

$$(S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4 \oplus b, S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus x_1,$$
$$S_6(S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus$$
$$\oplus (S_5(S_3(S_1(x_1) \oplus x_2 \oplus a) \oplus x_3) \oplus S_2(x_3) \oplus x_4 \oplus b, S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus x_1,$$
$$S_6(S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus x_1) \oplus S_1(x_1) \oplus x_2 \oplus a, S_3(S_1(x_1) \oplus x_2 \oplus a) \oplus x_3) =$$
$$= [S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus S_5(S_3(S_1(x_1) \oplus x_2 \oplus a) \oplus x_3) \oplus S_2(x_3),$$
$$S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus S_4(S_2(x_3) \oplus x_4 \oplus b), S_6(S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus x_1) \oplus$$
$$\oplus S_6(S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus x_1) \oplus S_1(x_1) \oplus S_1(x_1) \oplus a, S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus a \oplus$$
$$\oplus S_1(x_1))].$$

Таким чином, вектор $x = (x_1, x_2, x_3, x_4)$ задовольняє

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F(x_1 \parallel (x_2 \oplus a) \parallel x_3 \parallel (x_4 \oplus b)) = m \parallel c \parallel k \parallel d$$

тоді і тільки тоді, коли:

$$S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus S_5(S_3(S_1(x_1) \oplus x_2 \oplus a) \oplus x_3) \oplus S_2(x_3) = m$$

$$S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus S_4(S_2(x_3) \oplus x_4 \oplus b) = c$$

$$S_6(S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus x_1) \oplus S_6(S_4(S_2(x_3) \oplus x_4 \oplus b) \oplus x_1) \oplus S_1(x_1) \oplus S_1(x_1) \oplus a = k$$

$$S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus a \oplus S_1(x_1)) = d$$

що рівносильно

$$x_2 \oplus S_1(x_1) \in D_{S_3}(a \to d)$$

$$x_4 \oplus S_2(x_3) \in D_{S_4}(b \to c)$$

$$x_3 \oplus S_3(S_1(x_1) \oplus x_2) \in D_{S_5}(d \to b \oplus m)$$

$$x_1 \oplus S_4(S_2(x_3) \oplus x_4 \oplus b) \in D_{S_6}(c \to k \oplus a)$$

Таким чином доведено, що існує $\delta_{S_5}(d, b \oplus m)$ значень x_3, для кожного з яких існує $\delta_{S_4}(b, c)$ значень x_4 та для кожного з них $\delta_{S_6}(c, k \oplus a)$ значень x_1 та для кожного з них $\delta_{S_3}(a, d)$ значень x_2, таких що x досягає різниці.

Випадок 9.

Розглянемо проходження різниці входів x та $x \oplus (a||b||0||0)$ через функцію F таким чином, щоб одержати на виході різницю $(m||a||c||d)$.

Перший раунд:

$$(x_2 \oplus S_1(x_1), x_3, x_4 \oplus S_2(x_3), x_1) \oplus (x_2 \oplus S_1(x_1 \oplus a), x_3, x_4 \oplus S_2(x_3),$$
$$x_1 \oplus a) = [a \oplus S_1(x_1) \oplus S_1(x_1 \oplus a), b, \oplus S_2(x_3) \oplus S_2(x_3), c].$$

Другий раунд:

$$(S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_1(x_1) \oplus x_2) \oplus$$
$$\oplus (S_3(x_2 \oplus S_1(x_1 \oplus a)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1 \oplus a,$$
$$S_1(x_1 \oplus a) \oplus x_2) = [S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus S_1(x_1 \oplus a)), S_2(x_3) \oplus S_2(x_3),$$
$$S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3) \oplus x_4) \oplus a, a \oplus S_1(x_1) \oplus S_1(x_1 \oplus a)].$$

Третій раунд:

$$(S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_6(S_4(S_2(x_3) \oplus x_4) \oplus$$
$$\oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus (S_5(S_3(S_1(x_1 \oplus a) \oplus x_2) \oplus x_3) \oplus$$
$$\oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1 \oplus a, S_6(S_4(S_2(x_3) \oplus x_4) \oplus$$
$$\oplus x_1 \oplus a) \oplus S_1(x_1 \oplus a) \oplus x_2, S_3(S_1(x_1 \oplus a) \oplus x_2) \oplus x_3) = [S_5(S_3(S_1(x_1) \oplus x_2) \oplus$$
$$\oplus x_3) \oplus S_2(x_3) \oplus S_5(S_3(S_1(x_1 \oplus a) \oplus x_2) \oplus x_3) \oplus S_2(x_3), S_4(S_2(x_3) \oplus x_4) \oplus$$
$$\oplus S_4(S_2(x_3) \oplus x_4) \oplus a, S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_6(S_4(S_2(x_3) \oplus x_4) \oplus$$
$$\oplus x_1 \oplus a) \oplus S_1(x_1) \oplus S_1(x_1 \oplus a), S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus S_1(x_1 \oplus a))].$$

Таким чином, вектор $x = (x_1, x_2, x_3, x_4)$ задовольняє

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F((x_1 \oplus a) \parallel (x_2 \oplus b) \parallel x_3 \parallel x_4) = m \parallel a \parallel k \parallel d$$

тоді і тільки тоді, коли:

$$S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus S_5(S_3(S_1(x_1 \oplus a) \oplus x_2) \oplus x_3) \oplus S_2(x_3) = m$$

$$S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3) \oplus x_4) \oplus a = a$$

$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1 \oplus a) \oplus S_1(x_1) \oplus S_1(x_1 \oplus a) = c$$

$$S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus S_1(x_1 \oplus a)) = d$$

що рівносильно

$$x_2 \oplus S_1(x_1) \in D_{S_3}(z \to d)$$

$$x_1 \oplus S_4(S_2(x_3) \oplus x_4) \in D_{S_6}(a \to z \oplus c)$$

$$x_1 \in D_{S_1}(a \to z)$$

$$x_3 \oplus S_3(S_1(x_1) \oplus x_2) \in D_{S_5}(d \to m)$$

якщо S_1 – бієктвний.

Таким чином доведено, що для будь-якого фіксованого $z \in F_2^n$ таке, що існує $\delta_{S_1}(a, z)$ значень x_1, для кожного з яких існує $\delta_{S_3}(z, d)$ значень x_2 та для кожного з них $\delta_{S_5}(d, m)$ значень x_3, таких що x досягає різниці.

Випадок 10.

Розглянемо проходження різниці входів x та $x \oplus (0||0||a||b)$ через функцію F таким чином, щоб одержати на виході різницю $(m||d||c||a)$.

Перший раунд:

$$(x_2 \oplus S_1(x_1),x_3,x_4 \oplus S_2(x_3),x_1) \oplus (x_2 \oplus S_1(x_1),x_3 \oplus a,x_4 \oplus b \oplus S_2(x_3 \oplus a),$$
$$x_1) = [a \oplus S_1(x_1) \oplus S_1(x_1),b, \oplus S_2(x_3) \oplus S_2(x_3 \oplus a),c].$$

Другий раунд:

$$(S_3(x_2 \oplus S_1(x_1)) \oplus x_3, S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_1(x_1) \oplus x_2) \oplus$$
$$\oplus (S_3(x_2 \oplus S_1(x_1)) \oplus x_3 \oplus a, S_2(x_3 \oplus a) \oplus x_4 \oplus b, S_4(S_2(x_3 \oplus a) \oplus x_4 \oplus b) \oplus x_1,$$
$$S_1(x_1) \oplus x_2) = [S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus S_1(x_1)) \oplus a, S_2(x_3) \oplus S_2(x_3 \oplus a) \oplus b,$$
$$S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3 \oplus a) \oplus x_4 \oplus b), a \oplus S_1(x_1) \oplus S_1(x_1)].$$

Третій раунд:

$$(S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1, S_6(S_4(S_2(x_3) \oplus x_4) \oplus$$
$$\oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus (S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3 \oplus a) \oplus$$
$$\oplus S_2(x_3 \oplus a) \oplus x_4 \oplus b, S_4(S_2(x_3 \oplus a) \oplus x_4 \oplus b) \oplus x_1, S_6(S_4(S_2(x_3 \oplus a) \oplus x_4 \oplus b) \oplus$$
$$\oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3 \oplus a) = [S_5(S_3(S_1(x_1) \oplus x_2) \oplus$$

$$\oplus x_3) \oplus S_2(x_3) \oplus S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3 \oplus a) \oplus S_2(x_3 \oplus a) \oplus b, S_4(S_2(x_3) \oplus x_4) \oplus$$
$$\oplus S_4(S_2(x_3 \oplus a) \oplus x_4 \oplus b), S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_6(S_4(S_2(x_3 \oplus a) \oplus x_4 \oplus b) \oplus$$
$$\oplus x_1) \oplus S_1(x_1) \oplus S_1(x_1), S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus S_1(x_1)) \oplus a].$$

Таким чином, вектор $x = (x_1, x_2, x_3, x_4)$ задовольняє

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F(x_1 \parallel x_2 \parallel (x_3 \oplus a) \parallel (x_4 \oplus b)) = m \parallel d \parallel c \parallel a$$

тоді і тільки тоді, коли:

$$S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3 \oplus a) \oplus S_2(x_3 \oplus a) \oplus b = m$$

$$S_4(S_2(x_3) \oplus x_4) \oplus S_4(S_2(x_3 \oplus a) \oplus x_4 \oplus b) = d$$

$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_6(S_4(S_2(x_3 \oplus a) \oplus x_4 \oplus b) \oplus x_1) \oplus S_1(x_1) \oplus S_1(x_1) = c$$

$$S_3(x_2 \oplus S_1(x_1)) \oplus S_3(x_2 \oplus S_1(x_1)) \oplus a = a$$

що рівносильно

$$x_3 \in D_{S_2}(a \to z)$$

$$x_4 \oplus S_2(x_3) \in D_{S_4}(z \to d)$$

$$x_1 \oplus S_4(S_2(x_3) \oplus x_4) \in D_{S_6}(d \to c)$$

$$x_3 \oplus S_3(S_1(x_1) \oplus x_2) \in D_{S_5}(a \to m \oplus z)$$

якщо S_2 – бієктвний.

Таким чином доведено, що для будь-якого фіксованого $z \in F_2^n$ таке, що існує $\delta_{S_2}(a, z)$ значень x_3, для кожного з яких існує $\delta_{S_4}(z, d)$ значень x_4 та для кожного з них $\delta_{S_6}(d, c)$ значень x_1 та для кожного з них $\delta_{S_5}(a, m \oplus z)$ значень x_2, таких що x досягає різниці. □

Основний результат щодо оцінки диференціальної рівномірності без ключової схеми CLEFIA подамо у вигляді такої теореми.

Теорема 2.2. *Нехай S_1, S_2, S_3, S_4, S_5 та S_6 – це n-бітні S-блоки (не обов'язково різні), F – це $4n$-бітова функція, побудована за структурою*

трираундової схеми CLEFIA із відображеннями S_1, S_2, S_3, S_4, S_5 *та* S_6 *в якості раундових перетворень. Тоді,*

$$\delta(F) \geq \max(\delta(S_6)\delta\min(S_4), \delta(S_5)\delta\min(S_3)),$$

де $\delta\min(S) = min_{a\neq 0} max_b \delta_S(a,b)$.

Зокрема, якщо S_6 *є перестановкою:*

$$\delta(F) \geq \max_{i\neq 6, j\neq 6, i} \max(\delta(S_i)\delta_{min}(S_j), \delta(S_{i+1})\delta_{min}(S_6^{-1})),$$

якщо S_4 *не є перестановкою:*

$$\delta(F) \geq 2^{n+1}.$$

Доведення. Даний результат є прямим наслідком Теореми 2.1. Оскільки необхідно оцінювати кращі випадки, оберемо лише найменші значення диференціальної рівномірності та оцінемо їх. Доведемо наведену границю для першого випадку Теореми 2.1; інші випадки доводяться аналогічно.

Розглянемо диференціал (α,β), на якому S_4 досягає диференціальної рівномірності: $\delta(S_4) = \delta_{S_4}(\alpha,\beta)$. Оберемо $a = \alpha$ та якщо $b = \beta$; тоді для будь-яких $c \in V_n$

$$\delta_F(0 \parallel 0 \parallel 0 \parallel \alpha, \alpha \parallel \beta \parallel c \parallel 0) = \delta(S_4) \times \delta_{S_6}(\beta,c)$$

Тоді можемо вибрати для c значення, яке максимізує $\delta_{S_6}(\beta,c)$. Це значення завжди більше або дорівнює $\delta_{min}(S_6^{-1})$, якщо S_6 - бієктивний.

Так само розглянемо диференціал (α,β), на якому S_6 досягає диференціальної рівномірності: $\delta(S_6) = \delta_{S_6}(\alpha,\beta)$. Оберемо $b = \alpha$ та $c = \beta$; тоді для довільного $a \in V_n$:

$$\delta_F(0 \parallel 0 \parallel 0 \parallel a, a \parallel \alpha \parallel \beta \parallel 0) = \delta(S_6) \times \delta_{S_4}(a,\alpha).$$

Можемо вибрати для a значення, яке максимізує $\delta_{S_4}(a,\alpha)$. Це значення

завжди більше або дорівнює $\delta_{min}(S_4)$.

Припустимо тепер, що S_4 не бієктивний. Це означає, що існує деякий ненульовий $a \in V_n$: такий, що $\delta_{S_4}(a,0) \geq 0$. Тоді з першого пункту Теореми 2.1 випливає, що при $b = c = 0$ співвідношення

$$F(x_1 \parallel x_2 \parallel x_3 \parallel x_4) \oplus F(x_1 \parallel x_2 \parallel x_3 \parallel (x_4 \oplus a)) = (a,0,0,0)$$

має $\delta_{S_4}(a,0) \times \delta_{S_6}(0,0) \geq 2 \times 2^n = 2^{n+1}$ розв'язків у V_n^2 . □

2.2 Лінійні потенціали для трираундової схеми CLEFIA

Результати, аналогічні твердженням Теорем 2.1, також одержуються для лінійних потенціалів безключової трираундової схеми CLEFIA, що дозволяє виводити безпосередні оцінки стійкості до лінійного криптоаналізу.

Одержані оцінки нелінійності для трираундової схеми CLEFIA базуються на розгляданні окремих різниць, для яких вхідна різниця одного з раундових S-блоків дорівнює нулю.

Теорема 2.3. *Нехай S_1, S_2, S_3, S_4, S_5 та S_6 – це n-бітні S-блоки (не обов'язково різні), F – це $4n$-бітова функція, побудована за структурою трираундової схеми CLEFIA із відображеннями S_1, S_2, S_3, S_4, S_5 та S_6 в якості раундових перетворень. Тоді для будь-яких a, b,c,d,e, m, p та k з F_2^n маємо:*

1) Якщо S_4 та S_5 – бієктивні, то

$$\lambda_F(0||0||0||a,b||a||a||c) = \lambda_{S_4}(a,b) \times \lambda_{S_5}(a,b \oplus c)$$

2) Якщо S_2 та S_5 – бієктивні, то

$$\lambda_F(0||0||a||0,0||b||b||c) = \lambda_{S_2}(a,b) \times \lambda_{S_5}(b,c)$$

3) Якщо S_3 – бієктивний, то

$$\lambda_F(0||a||0||0,a||c||b||a) = \lambda_{S_3}(a,b) \times \lambda_{S_6}(a,b \oplus c)$$

4) Якщо S_1 та S_6 – бієктивні, то

$$\lambda_F(a||0||0||0,b||c||0||b) = \lambda_{S_1}(a,b) \times \lambda_{S_6}(b,c)$$

5) Якщо S_2 – бієктивний, то

$$\lambda_F(0||a||b||c,k||m||e||p) = \lambda_{S_2}(b,d) \times \lambda_{S_3}(a,c \oplus d \oplus e) \times \lambda_{S_4}(c,k \oplus a) \times$$
$$\times \lambda_{S_5}(d \oplus c, p \oplus k) \times \lambda_{S_6}(a, m \oplus e)$$

6) Якщо S_1 – бієктивний, то

$$\lambda_F(c||a||0||b,e||p||k||m) = \lambda_{S_1}(c,d) \times \lambda_{S_3}(a,k \oplus b) \times \lambda_{S_4}(b,e \oplus a \oplus d) \times$$
$$\times \lambda_{S_5}(b, m \oplus e) \times \lambda_{S_6}(d \oplus a, p \oplus k)$$

7) Якщо S_3 та S_4 – бієктивні, то

$$\lambda_F(p||m||k||a,b||c||d||e) = \lambda_{S_3}(m,d \oplus r) \times \lambda_{S_4}(a,b \oplus q) \times$$
$$\times \lambda_{S_5}(r, b \oplus e) \times \lambda_{S_6}(q, d \oplus e)$$

8) Якщо S_4 – бієктивний, то

$$\lambda_F(0||a||0||b,d||e||c||m) = \lambda_{S_3}(a,b \oplus c) \times \lambda_{S_4}(b,d \oplus a) \times$$
$$\times \lambda_{S_5}(b, m \oplus d) \times \lambda_{S_6}(a, e \oplus c)$$

9) Якщо S_1 – бієктивний, то

$$\lambda_F(a||b||0||0,d||m||k||d) = \lambda_{S_1}(a,q \oplus b) \times \lambda_{S_3}(b,k) \times \lambda_{S_6}(q, k \oplus m)$$

10) Якщо S_2 – бієктивний, то

$$\lambda_F(0||0||a||b,k||e||e||p) = \lambda_{S_2}(a,q) \times \lambda_{S_4}(b,k) \times \lambda_{S_5}(q, p \oplus k)$$

11) Якщо S_1 та S_2 – бієктивні, то

$$\lambda_F(a||0||b||0,c||k||d||e) = \lambda_{S_1}(a,c) \times \lambda_{S_2}(b,d) \times \lambda_{S_5}(d, e \oplus c) \times \lambda_{S_6}(c, d \oplus k)$$

12) Якщо S_4 – бієктивний, то

$$\lambda_F(a||0||b||c,k||p||e||m) = \lambda_{S_1}(a,d) \times \lambda_{S_2}(b,e \oplus c) \times \lambda_{S_4}(c,k \oplus d) \times$$
$$\times \lambda_{S_5}(e, m \oplus k) \times \lambda_{S_6}(d, p \oplus e)$$

13) Якщо S_3 – бієктивний, то

$$\lambda_F(a||b||c||0,d||m||k||p) = \lambda_{S_1}(a,d \oplus b) \times \lambda_{S_2}(c,e) \times \lambda_{S_3}(b,k \oplus e) \times$$
$$\times \lambda_{S_5}(e, p \oplus d) \times \lambda_{S_6}(d, k \oplus m)$$

Доведення.

$$F = [S_5(S_3(S_1(x_1) \oplus x_2) \oplus x_3) \oplus S_2(x_3) \oplus x_4, S_4(S_2(x_3) \oplus x_4) \oplus x_1,$$
$$S_6(S_4(S_2(x_3) \oplus x_4) \oplus x_1) \oplus S_1(x_1) \oplus x_2, S_3(S_1(x_1) \oplus x_2) \oplus x_3]$$

Випадок 1.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (0||0||0||a)$ через

функцію F таким чином, щоб одержати на виході пару $(b||a||a||c)$.

$$\lambda_F(0||0||0||a,b||a||a||c) =$$
$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{b\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus b\cdot S_2(x_3)\oplus b\cdot x_4\oplus a\cdot S_4(S_2(x_3)\oplus x_4)\oplus a\cdot x_1}\cdot$$
$$\cdot (-1)^{a\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)\oplus a\cdot S_1(x_1)\oplus a\cdot x_2\oplus a\cdot S_3(S_1(x_1)\oplus x_2)\oplus a\cdot x_3\cdot x_1\cdot x_2\cdot x_3\oplus a\cdot x_4} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(0\oplus a)\cdot(x_1\oplus a)\cdot S_1(x_1)\oplus(a)\cdot x_2\oplus a\cdot S_3(S_1(x_1)\oplus x_2)\oplus(c)\cdot x_3\oplus b\cdot S_2(x_3)\oplus}\cdot$$
$$\cdot (-1)^{b\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus(a\oplus b)\cdot x_4\oplus a\cdot S_4(S_2(x_3)\oplus x_4)\oplus a\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{b\cdot 0\oplus a\cdot S_4(0)\oplus(0\oplus a)\cdot(x_1\oplus a)\cdot S_6(S_4(0)\oplus x_1)\oplus a\cdot 0\oplus a\cdot S_3(0)\oplus(c)\cdot x_3\oplus}\cdot$$
$$\cdot (-1)^{b\cdot S_5(S_3(0)\oplus x_3)\oplus a\cdot 0\oplus a\cdot S_2(x_3)\cdot 0\cdot S_1(x_1)} = \lambda_{S_4}(a,b)\times\lambda_{S_5}(a,b\oplus c)$$

Випадок 2.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x\oplus(0||0||a||0)$ через функцію F таким чином, щоб одержати на виході пару $(0||b||b||c)$.

Якщо S_2 – бієктивний, тоді y приймає усі можливі позитивні значення з F_2^n, та $x_3 = S_3^{-1}(x_2\oplus y)$, тоді

$$\lambda_F(0||0||a||0,0||b||b||c) =$$
$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{0\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus 0\cdot S_2(x_3)\oplus 0\cdot x_4\oplus b\cdot S_4(S_2(x_3)\oplus x_4)\oplus b\cdot x_1}\cdot$$
$$\cdot (-1)^{b\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)\oplus b\cdot S_1(x_1)\oplus b\cdot x_2\oplus b\cdot S_3(S_1(x_1)\oplus x_2)\oplus b\cdot x_3\cdot x_1\cdot x_2\oplus a\cdot x_3\cdot x_4} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(0\oplus b)\cdot x_1\oplus b\cdot S_1(x_1)\oplus(b)\cdot x_2\oplus c\cdot S_3(S_1(x_1)\oplus x_2)\oplus(c\oplus a)\cdot x_3\oplus 0\cdot S_2(x_3)\oplus}\cdot$$
$$\cdot (-1)^{0\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus(0\oplus 0)\cdot x_4\oplus b\cdot S_4(S_2(x_3)\oplus x_4)\oplus b\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{0\cdot y\oplus b\cdot S_4(y)\oplus(0\oplus b)\cdot x_1\oplus b\cdot S_6(S_4(y)\oplus x_1)\oplus b\cdot 0\oplus c\cdot S_3(0)\oplus(c\oplus a)\cdot x_3\oplus}\cdot$$
$$\cdot (-1)^{0\cdot S_5(S_3(0)\oplus x_3)\cdot y\cdot S_2(x_3)\cdot 0\cdot S_1(x_1)} = \lambda_{S_2}(a,b)\times\lambda_{S_5}(b,c)$$

Випадок 3.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (0||a||0||0)$ через функцію F таким чином, щоб одержати на виході пару $(a||c||b||a)$.

$$\lambda_F(0||a||0||0,a||c||b||a) =$$
$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{a\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus a\cdot S_2(x_3)\oplus a\cdot x_4\oplus c\cdot S_4(S_2(x_3)\oplus x_4)\oplus c\cdot x_1}\cdot$$
$$\cdot (-1)^{b\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)\oplus b\cdot S_1(x_1)\oplus b\cdot x_2\oplus b\cdot S_3(S_1(x_1)\oplus x_2)\oplus b\cdot x_3\oplus 0\cdot x_1\oplus a\cdot x_2\oplus 0\cdot x_3\oplus 0\cdot x_4} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(0\oplus c)\cdot x_1\oplus b\cdot S_1(x_1)\oplus(b\oplus a)\cdot x_2\oplus a\cdot S_3(S_1(x_1)\oplus x_2)\oplus(a\oplus 0)\cdot x_3\oplus a\cdot S_2(x_3)\oplus}\cdot$$
$$\cdot (-1)^{a\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus(0\oplus a)\cdot x_4\oplus c\cdot S_4(S_2(x_3)\oplus x_4)\oplus b\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{a\cdot y\oplus c\cdot S_4(y)\oplus(0\oplus c)\cdot x_1\oplus b\cdot S_6(S_4(y)\oplus x_1)\oplus b\cdot 0\oplus a\cdot S_3(0)\oplus(a\oplus 0)\cdot x_3\oplus}\cdot$$
$$\cdot (-1)^{a\cdot S_5(S_3(0)\oplus x_3)\oplus 0\cdot y\oplus 0\cdot S_2(x_3)\oplus a\cdot 0\oplus a\cdot S_1(x_1)} = \lambda_{S_3}(a,b) \times \lambda_{S_6}(a,b\oplus c)$$

Випадок 4.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (a||0||0||0)$ через функцію F таким чином, щоб одержати на виході пару $(b||c||0||b)$.

Якщо S_1 – бієктивний, тоді a приймає усі можливі позитивні значення з F_2^n, та $S_1(x_1) \oplus x_2 = z$, тоді

$$\lambda_F(a||0||0||0,b||c||0||b) =$$
$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{b\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus b\cdot S_2(x_3)\oplus b\cdot x_4\oplus c\cdot S_4(S_2(x_3)\oplus x_4)\oplus c\cdot x_1}\cdot$$
$$\cdot (-1)^{0\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)\oplus 0\cdot S_1(x_1)\oplus 0\cdot x_2\oplus 0\cdot S_3(S_1(x_1)\oplus x_2)\oplus 0\cdot x_3\oplus a\cdot x_1\oplus 0\cdot x_2\oplus 0\cdot x_3\oplus 0\cdot x_4} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(a\oplus c)\cdot x_1\oplus 0\cdot S_1(x_1)\oplus(0\oplus 0)\cdot x_2\oplus b\cdot S_3(S_1(x_1)\oplus x_2)\oplus(b\oplus 0)\cdot x_3\oplus b\cdot S_2(x_3)\oplus}\cdot$$
$$\cdot (-1)^{b\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus(0\oplus b)\cdot x_4\oplus c\cdot S_4(S_2(x_3)\oplus x_4)\oplus 0\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)} =$$

$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{b\cdot 0\oplus c\cdot S_4(0)\oplus(a\oplus c)\cdot x_1\oplus 0\cdot S_6(S_4(0)\oplus x_1)\oplus 0\cdot z\oplus b\cdot S_3(z)\oplus(b\oplus 0)\cdot x_3\oplus} \cdot$$

$$\cdot (-1)^{b\cdot S_5(S_3(z)\oplus x_3)\oplus 0\cdot 0\oplus 0\cdot S_2(x_3)\oplus 0\cdot z\oplus 0\cdot S_1(x_1)} = \lambda_{S_1}(a,b) \times \lambda_{S_6}(b,c)$$

Випадок 5.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (0||a||b||c)$ через функцію F таким чином, щоб одержати на виході пару $(k||m||e||p)$.

Якщо S_2 – бієктивний, тоді y приймає усі можливі позитивні значення з F_2^n, та $S_2(x_3) \oplus x_4 = y$, тоді

$$\lambda_F(0||a||b||c,k||m||e||p) =$$

$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{k\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus k\cdot S_2(x_3)\oplus k\cdot x_4\oplus m\cdot S_4(S_2(x_3)\oplus x_4)\oplus m\cdot x_1}\cdot$$

$$\cdot (-1)^{e\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)\oplus e\cdot S_1(x_1)\oplus e\cdot x_2\oplus e\cdot S_3(S_1(x_1)\oplus x_2)\oplus e\cdot x_3\oplus 0\cdot x_1\oplus a\cdot x_2\oplus b\cdot x_3\oplus c\cdot x_4} =$$

$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(0\oplus m)\cdot x_1\oplus e\cdot S_1(x_1)\oplus(e\oplus a)\cdot x_2\oplus p\cdot S_3(S_1(x_1)\oplus x_2)\oplus(p\oplus b)\cdot x_3\oplus k\cdot S_2(x_3)\oplus}\cdot$$

$$\cdot (-1)^{k\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus(c\oplus k)\cdot x_4\oplus m\cdot S_4(S_2(x_3)\oplus x_4)\oplus e\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)} =$$

$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{k\cdot y\oplus m\cdot S_4(y)\oplus(0\oplus m)\cdot x_1\oplus e\cdot S_6(S_4(y)\oplus x_1)\oplus e\cdot 0\oplus p\cdot S_3(0)\oplus(p\oplus b)\cdot x_3\oplus}\cdot$$

$$\cdot(-1)^{k\cdot S_5(S_3(0)\oplus x_3)\oplus c\cdot y\oplus c\cdot S_2(x_3)\oplus a\cdot 0\oplus a\cdot S_1(x_1)} = \lambda_{S_2}(b,d)\times\lambda_{S_3}(a,c\oplus d\oplus e)\times\lambda_{S_4}(c,k\oplus a)\times$$

$$\times \lambda_{S_5}(d\oplus c, p\oplus k) \times \lambda_{S_6}(a, m\oplus e)$$

Випадок 6.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (c||a||0||b)$ через функцію F таким чином, щоб одержати на виході пару $(e||p||k||m)$.

Якщо S_1 – бієктивний, тоді z приймає усі можливі позитивні значення

з F_2^n, та $S_1(x_1) \oplus x_2 = z$, тоді

$$\lambda_F(c||a||0||b,e||p||k||m) =$$
$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{e\cdot S_5(S_3(S_1(e_1)\oplus e_2)\oplus e_3)\oplus e\cdot S_2(e_3)\oplus e\cdot e_4\oplus p\cdot S_4(S_2(e_3)\oplus e_4)\oplus p\cdot e_1}\cdot$$
$$\cdot (-1)^{k\cdot S_6(S_4(S_2(e_3)\oplus e_4)\oplus e_1)\oplus k\cdot S_1(e_1)\oplus k\cdot e_2\oplus k\cdot S_3(S_1(e_1)\oplus e_2)\oplus k\cdot e_3\oplus c\cdot e_1\oplus a\cdot e_2\oplus 0\cdot e_3\oplus b\cdot e_4} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(c\oplus p)\cdot e_1\oplus k\cdot S_1(e_1)\oplus(k\oplus a)\cdot e_2\oplus m\cdot S_3(S_1(e_1)\oplus e_2)\oplus(m\oplus 0)\cdot e_3\oplus e\cdot S_2(e_3)\oplus}\cdot$$
$$\cdot (-1)^{e\cdot S_5(S_3(S_1(e_1)\oplus e_2)\oplus e_3)\oplus(b\oplus e)\cdot e_4\oplus p\cdot S_4(S_2(e_3)\oplus e_4)\oplus k\cdot S_6(S_4(S_2(e_3)\oplus e_4)\oplus e_1)} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{e\cdot 0\oplus p\cdot S_4(0)\oplus(c\oplus p)\cdot e_1\oplus k\cdot S_6(S_4(0)\oplus e_1)\oplus k\cdot z\oplus m\cdot S_3(z)\oplus(m\oplus 0)\cdot e_3\oplus}\cdot$$
$$\cdot(-1)^{e\cdot S_5(S_3(z)\oplus e_3)\oplus b\cdot 0\oplus b\cdot S_2(e_3)\oplus a\cdot z\oplus a\cdot S_1(e_1)} = \lambda_{S_1}(c,d)\times\lambda_{S_3}(a,k\oplus b)\times\lambda_{S_4}(b,e\oplus a\oplus d)\times$$
$$\times\,\lambda_{S_5}(b,m\oplus e)\times\lambda_{S_6}(d\oplus a,p\oplus k)$$

Випадок 7.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x\oplus(p||m||k||a)$ через функцію F таким чином, щоб одержати на виході пару $(b||c||d||e)$.

Якщо S_1 – бієктивний, тоді z приймає усі можливі позитивні значення з F_2^n, та $S_1(x_1) \oplus x_2 = z$, тоді

$$\lambda_F(p||m||k||a,b||c||d||e) =$$
$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{b\cdot S_5(S_3(S_1(b_1)\oplus b_2)\oplus b_3)\oplus b\cdot S_2(b_3)\oplus b\cdot b_4\oplus c\cdot S_4(S_2(b_3)\oplus b_4)\oplus c\cdot b_1}\cdot$$
$$\cdot (-1)^{d\cdot S_6(S_4(S_2(b_3)\oplus b_4)\oplus b_1)\oplus d\cdot S_1(b_1)\oplus d\cdot b_2\oplus d\cdot S_3(S_1(b_1)\oplus b_2)\oplus d\cdot b_3\oplus p\cdot b_1\oplus m\cdot b_2\oplus k\cdot b_3\oplus a\cdot b_4} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(p\oplus c)\cdot b_1\oplus d\cdot S_1(b_1)\oplus(d\oplus m)\cdot b_2\oplus e\cdot S_3(S_1(b_1)\oplus b_2)\oplus(e\oplus k)\cdot b_3\oplus b\cdot S_2(b_3)\oplus}\cdot$$
$$\cdot (-1)^{b\cdot S_5(S_3(S_1(b_1)\oplus b_2)\oplus b_3)\oplus(a\oplus b)\cdot b_4\oplus c\cdot S_4(S_2(b_3)\oplus b_4)\oplus d\cdot S_6(S_4(S_2(b_3)\oplus b_4)\oplus b_1)} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{b\cdot y\oplus c\cdot S_4(y)\oplus(p\oplus c)\cdot b_1\oplus d\cdot S_6(S_4(y)\oplus b_1)\oplus d\cdot z\oplus e\cdot S_3(z)\oplus(e\oplus k)\cdot b_3\oplus}\cdot$$
$$\cdot (-1)^{b\cdot S_5(S_3(z)\oplus b_3)\oplus a\cdot y\oplus a\cdot S_2(b_3)\oplus m\cdot z\oplus m\cdot S_1(b_1)}$$

Якщо S_2 – бієктивний, тоді y приймає усі можливі позитивні значення з F_2^n, та $S_2(x_3) \oplus x_4 = y$, тоді

$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{b\cdot y\oplus c\cdot S_4(y)\oplus(p\oplus c)\cdot b_1\oplus d\cdot S_6(S_4(y)\oplus b_1)\oplus d\cdot z\oplus e\cdot S_3(z)\oplus(e\oplus k)\cdot b_3\oplus}.$$

$$\cdot\,(-1)^{b\cdot S_5(S_3(z)\oplus b_3)\oplus a\cdot y\oplus a\cdot S_2(b_3)\oplus m\cdot z\oplus m\cdot S_1(b_1)} =$$

$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(b\oplus a)\cdot y\oplus c\cdot S_4(y)} \cdot \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(p\oplus c)\cdot x_1\oplus m\cdot S_1(x_1)\oplus d\cdot S_6(S_4(y)\oplus x_1)}.$$

$$\cdot \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(d\oplus m)\cdot z\oplus e\cdot S_3(z)} \cdot \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^2} (-1)^{(e\oplus k)\cdot x_3\oplus a\cdot S_2(x_3)\oplus b\cdot S_5(S_3(z)\oplus x_3)} =$$

$$= \lambda_{S_3}(m,d\oplus r) \times \lambda_{S_4}(a,b\oplus q) \times \lambda_{S_5}(r,b\oplus e) \times \lambda_{S_6}(q,d\oplus e)$$

Випадок 8.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (0||a||0||b)$ через функцію F таким чином, щоб одержати на виході пару $(d||e||c||m)$.

$$\lambda_F(0||a||0||b,d||e||c||m) =$$

$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{d\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus d\cdot S_2(x_3)\oplus d\cdot x_4\oplus e\cdot S_4(S_2(x_3)\oplus x_4)\oplus e\cdot x_1}.$$

$$\cdot\,(-1)^{c\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)\oplus c\cdot S_1(x_1)\oplus c\cdot x_2\oplus c\cdot S_3(S_1(x_1)\oplus x_2)\oplus c\cdot x_3\oplus 0\cdot x_1\oplus a\cdot x_2\oplus 0\cdot x_3\oplus b\cdot x_4} =$$

$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(0\oplus e)\cdot x_1\oplus c\cdot S_1(x_1)\oplus(c\oplus a)\cdot x_2\oplus m\cdot S_3(S_1(x_1)\oplus x_2)\oplus(m\oplus 0)\cdot x_3\oplus d\cdot S_2(x_3)\oplus}.$$

$$\cdot\,(-1)^{d\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus(b\oplus d)\cdot x_4\oplus e\cdot S_4(S_2(x_3)\oplus x_4)\oplus c\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)} =$$

$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{d\cdot y\oplus e\cdot S_4(y)\oplus(0\oplus e)\cdot x_1\oplus c\cdot S_6(S_4(y)\oplus x_1)\oplus c\cdot 0\oplus m\cdot S_3(0)\oplus(m\oplus 0)\cdot x_3\oplus}.$$

$$\cdot\,(-1)^{d\cdot S_5(S_3(0)\oplus x_3)\oplus b\cdot y\oplus b\cdot S_2(x_3)\oplus a\cdot 0\oplus a\cdot S_1(x_1)} = \lambda_{S_3}(a,b\oplus c) \times \lambda_{S_4}(b,d\oplus a)\times$$

$$\times \lambda_{S_5}(b,m\oplus d) \times \lambda_{S_6}(a,e\oplus c)$$

Випадок 9.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (a||b||0||0)$ через

функцію F таким чином, щоб одержати на виході пару $(d||m||k||d)$.

Якщо S_1 – бієктивний, тоді z приймає усі можливі позитивні значення з F_2^n, та $S_1(x_1) \oplus x_2 = z$, тоді

$$\lambda_F(a||b||0||0,d||m||k||d) =$$
$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{d\cdot S_5(S_3(S_1(d_1)\oplus d_2)\oplus d_3)\oplus d\cdot S_2(d_3)\oplus d\cdot d_4\oplus m\cdot S_4(S_2(d_3)\oplus d_4)\oplus m\cdot d_1}.$$
$$\cdot (-1)^{k\cdot S_6(S_4(S_2(d_3)\oplus d_4)\oplus d_1)\oplus k\cdot S_1(d_1)\oplus k\cdot d_2\oplus k\cdot S_3(S_1(d_1)\oplus d_2)\oplus k\cdot d_3\oplus a\cdot d_1\oplus b\cdot d_2\oplus 0\cdot d_3\oplus 0\cdot d_4} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(a\oplus m)\cdot d_1\oplus k\cdot S_1(d_1)\oplus(k\oplus b)\cdot d_2\oplus d\cdot S_3(S_1(d_1)\oplus d_2)\oplus(d\oplus 0)\cdot d_3\oplus d\cdot S_2(d_3)\oplus}.$$
$$\cdot (-1)^{d\cdot S_5(S_3(S_1(d_1)\oplus d_2)\oplus d_3)\oplus(0\oplus d)\cdot d_4\oplus m\cdot S_4(S_2(d_3)\oplus d_4)\oplus k\cdot S_6(S_4(S_2(d_3)\oplus d_4)\oplus d_1)} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{d\cdot y\oplus m\cdot S_4(y)\oplus(a\oplus m)\cdot d_1\oplus k\cdot S_6(S_4(y)\oplus d_1)\oplus k\cdot z\oplus d\cdot S_3(z)\oplus(d\oplus 0)\cdot d_3\oplus}.$$
$$\cdot (-1)^{d\cdot S_5(S_3(z)\oplus d_3)\oplus 0\cdot y\oplus 0\cdot S_2(d_3)\oplus b\cdot z\oplus b\cdot S_1(d_1)} =$$
$$= \lambda_{S_1}(a,q\oplus b)\times\lambda_{S_3}(b,k)\times\lambda_{S_6}(q,k\oplus m)$$

Випадок 10.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (0||0||a||b)$ через функцію F таким чином, щоб одержати на виході пару $(k||e||e||p)$.

Якщо S_2 – бієктивний, тоді y приймає усі можливі позитивні значення з F_2^n, та $S_2(x_3) \oplus x_4 = y$, тоді

$$\lambda_F(0||0||a||b,k||e||e||p) =$$
$$(x_1,x_2,x_3,x_4)\in(F_2^n)^4 (-1)^{k\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus k\cdot S_2(x_3)\oplus k\cdot x_4\oplus e\cdot S_4(S_2(x_3)\oplus x_4)\oplus e\cdot x_1}.$$
$$\cdot (-1)^{e\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)\oplus e\cdot S_1(x_1)\oplus e\cdot x_2\oplus e\cdot S_3(S_1(x_1)\oplus x_2)\oplus e\cdot x_3\oplus 0\cdot x_1\oplus 0\cdot x_2\oplus a\cdot x_3\oplus b\cdot x_4} =$$
$$=_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(0\oplus e)\cdot x_1\oplus e\cdot S_1(x_1)\oplus(e\oplus 0)\cdot x_2\oplus p\cdot S_3(S_1(x_1)\oplus x_2)\oplus(p\oplus a)\cdot x_3\oplus k\cdot S_2(x_3)\oplus}.$$
$$\cdot (-1)^{k\cdot S_5(S_3(S_1(x_1)\oplus x_2)\oplus x_3)\oplus(b\oplus k)\cdot x_4\oplus e\cdot S_4(S_2(x_3)\oplus x_4)\oplus e\cdot S_6(S_4(S_2(x_3)\oplus x_4)\oplus x_1)} =$$
$$=_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{k\cdot y\oplus e\cdot S_4(y)\oplus(0\oplus e)\cdot x_1\oplus e\cdot S_6(S_4(y)\oplus x_1)\oplus e\cdot 0\oplus p\cdot S_3(0)\oplus(p\oplus a)\cdot x_3\oplus}.$$
$$\cdot (-1)^{k\cdot S_5(S_3(0)\oplus x_3)\oplus b\cdot y\oplus b\cdot S_2(x_3)\oplus 0\cdot 0\oplus 0\cdot S_1(x_1)} = \lambda_{S_2}(a,q)\times\lambda_{S_4}(b,k)\times\lambda_{S_5}(q,p\oplus k)$$

Випадок 11.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (a||0||b||0)$ через функцію F таким чином, щоб одержати на виході пару $(d||m||k||p)$.

Якщо S_1 – бієктивний, тоді z приймає усі можливі позитивні значення з F_2^n, та $S_1(x_1) \oplus x_2 = z$ та якщо S_2 – бієктивний, тоді y приймає усі можливі позитивні значення з F_2^n, та $S_2(x_3) \oplus x_4 = y$, тоді

$$\lambda_F(a||0||b||0,c||k||d||e) =$$
$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{c\cdot S_5(S_3(S_1(c_1)\oplus c_2)\oplus c_3)\oplus c\cdot S_2(c_3)\oplus c\cdot c_4\oplus k\cdot S_4(S_2(c_3)\oplus c_4)\oplus k\cdot c_1}\cdot$$
$$\cdot (-1)^{d\cdot S_6(S_4(S_2(c_3)\oplus c_4)\oplus c_1)\oplus d\cdot S_1(c_1)\oplus d\cdot c_2\oplus d\cdot S_3(S_1(c_1)\oplus c_2)\oplus d\cdot c_3\oplus a\cdot c_1\oplus 0\cdot c_2\oplus b\cdot c_3\oplus 0\cdot c_4} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(a\oplus k)\cdot c_1\oplus d\cdot S_1(c_1)\oplus(d\oplus 0)\cdot c_2\oplus e\cdot S_3(S_1(c_1)\oplus c_2)\oplus(e\oplus b)\cdot c_3\oplus c\cdot S_2(c_3)\oplus}\cdot$$
$$\cdot (-1)^{c\cdot S_5(S_3(S_1(c_1)\oplus c_2)\oplus c_3)\oplus(0\oplus c)\cdot c_4\oplus k\cdot S_4(S_2(c_3)\oplus c_4)\oplus d\cdot S_6(S_4(S_2(c_3)\oplus c_4)\oplus c_1)} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{c\cdot y\oplus k\cdot S_4(y)\oplus(a\oplus k)\cdot c_1\oplus d\cdot S_6(S_4(y)\oplus c_1)\oplus d\cdot z\oplus e\cdot S_3(z)\oplus(e\oplus b)\cdot c_3\oplus}\cdot$$
$$\cdot (-1)^{c\cdot S_5(S_3(z)\oplus c_3)\oplus 0\cdot y\oplus 0\cdot S_2(c_3)\oplus 0\cdot z\oplus 0\cdot S_1(c_1)} =$$
$$= \lambda_{S_1}(a,c) \times \lambda_{S_2}(b,d) \times \lambda_{S_5}(d, e\oplus c) \times \lambda_{S_6}(c, d\oplus k)$$

Випадок 12.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (a||0||b||c)$ через функцію F таким чином, щоб одержати на виході пару $(k||p||e||m)$.

Якщо S_1 – бієктивний, тоді z приймає усі можливі позитивні значення з F_2^n, та $S_1(x_1) \oplus x_2 = z$ та якщо S_2 – бієктивний, тоді y приймає усі можливі

позитивні значення з F_2^n, та $S_2(x_3) \oplus x_4 = y$, тоді

$$\lambda_F(a||0||b||c,k||p||e||m) =$$
$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{k\cdot S_5(S_3(S_1(k_1)\oplus k_2)\oplus k_3)\oplus k\cdot S_2(k_3)\oplus k\cdot k_4\oplus p\cdot S_4(S_2(k_3)\oplus k_4)\oplus p\cdot k_1}\cdot$$
$$\cdot (-1)^{e\cdot S_6(S_4(S_2(k_3)\oplus k_4)\oplus k_1)\oplus e\cdot S_1(k_1)\oplus e\cdot k_2\oplus e\cdot S_3(S_1(k_1)\oplus k_2)\oplus e\cdot k_3\oplus a\cdot k_1\oplus 0\cdot k_2\oplus b\cdot k_3\oplus c\cdot k_4} =$$
$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(a\oplus p)\cdot k_1\oplus e\cdot S_1(k_1)\oplus(e\oplus 0)\cdot k_2\oplus m\cdot S_3(S_1(k_1)\oplus k_2)\oplus(m\oplus b)\cdot k_3\oplus k\cdot S_2(k_3)\oplus}\cdot$$
$$\cdot (-1)^{k\cdot S_5(S_3(S_1(k_1)\oplus k_2)\oplus k_3)\oplus(c\oplus k)\cdot k_4\oplus p\cdot S_4(S_2(k_3)\oplus k_4)\oplus e\cdot S_6(S_4(S_2(k_3)\oplus k_4)\oplus k_1)} =$$

$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{k\cdot y\oplus p\cdot S_4(y)\oplus(a\oplus p)\cdot k_1\oplus e\cdot S_6(S_4(y)\oplus k_1)\oplus e\cdot z\oplus m\cdot S_3(z)\oplus(m\oplus b)\cdot k_3\oplus}\cdot$$
$$\cdot (-1)^{k\cdot S_5(S_3(z)\oplus k_3)\oplus c\cdot y\oplus c\cdot S_2(k_3)\oplus 0\cdot z\oplus 0\cdot S_1(k_1)} =$$
$$= \lambda_{S_1}(a,d) \times \lambda_{S_2}(b,e\oplus c) \times \lambda_{S_4}(c,k\oplus d) \times \lambda_{S_5}(e,m\oplus k) \times \lambda_{S_6}(d,p\oplus e)$$

Випадок 13.

Для вектору $x \in V_n^2$ позначимо через x_1, x_2, x_3 та x_4 його частини відповідно. Розглянемо проходження пари входів x та $x \oplus (a||b||c||0)$ через функцію F таким чином, щоб одержати на виході пару $(d||m||k||p)$.

Якщо S_1 – бієктивний, тоді z приймає усі можливі позитивні значення з F_2^n, та $S_1(x_1)\oplus x_2 = z$ та якщо S_2 – бієктивний, тоді y приймає усі можливі позитивні значення з F_2^n, та $S_2(x_3) \oplus x_4 = y$, тоді

$$\lambda_F(a||b||c||0,d||m||k||p) =$$
$$\sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{d\cdot S_5(S_3(S_1(d_1)\oplus d_2)\oplus d_3)\oplus d\cdot S_2(d_3)\oplus d\cdot d_4\oplus m\cdot S_4(S_2(d_3)\oplus d_4)\oplus m\cdot d_1}\cdot$$
$$\cdot (-1)^{k\cdot S_6(S_4(S_2(d_3)\oplus d_4)\oplus d_1)\oplus k\cdot S_1(d_1)\oplus k\cdot d_2\oplus k\cdot S_3(S_1(d_1)\oplus d_2)\oplus k\cdot d_3\oplus a\cdot d_1\oplus b\cdot d_2\oplus c\cdot d_3\oplus 0\cdot d_4} =$$

$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{(a\oplus m)\cdot d_1\oplus k\cdot S_1(d_1)\oplus(k\oplus b)\cdot d_2\oplus p\cdot S_3(S_1(d_1)\oplus d_2)\oplus(p\oplus c)\cdot d_3\oplus d\cdot S_2(d_3)\oplus}.$$

$$\cdot (-1)^{d\cdot S_5(S_3(S_1(d_1)\oplus d_2)\oplus d_3)\oplus(0\oplus d)\cdot d_4\oplus m\cdot S_4(S_2(d_3)\oplus d_4)\oplus k\cdot S_6(S_4(S_2(d_3)\oplus d_4)\oplus d_1)} =$$

$$= \sum_{(x_1,x_2,x_3,x_4)\in(F_2^n)^4} (-1)^{d\cdot y\oplus m\cdot S_4(y)\oplus(a\oplus m)\cdot d_1\oplus k\cdot S_6(S_4(y)\oplus d_1)\oplus k\cdot z\oplus p\cdot S_3(z)\oplus(p\oplus c)\cdot d_3\oplus}.$$

$$\cdot (-1)^{d\cdot S_5(S_3(z)\oplus d_3)\oplus 0\cdot y\oplus 0\cdot S_2(d_3)\oplus b\cdot z\oplus b\cdot S_1(d_1)} =$$

$$= \lambda_{S_1}(a,d\oplus b)\times\lambda_{S_2}(c,e)\times\lambda_{S_3}(b,k\oplus e)\times\lambda_{S_5}(e,p\oplus d)\times\lambda_{S_6}(d,k\oplus m)$$

□

Основний результат щодо оцінки лінійних потенціалів безключової схеми CLEFIA подамо у вигляді такої теореми.

Теорема 2.4. *Нехай S_1 , S_2, S_3, S_4, S_5, та S_6 – це n-бітні S-блоки (не обов'язково різні), F – це $4n$-бітова функція, побудована за структурою трираундової схеми CLEFIA із відображеннями S_1 , S_2, S_3, S_4, S_5, та S_6 в якості раундових перетворень. Тоді:*

$$\mathcal{L}(F) \geq \max(\mathcal{L}(S_4)\mathcal{L}_{min}(S_5),\mathcal{L}(S_2)\mathcal{L}_{min}(S_5),\mathcal{L}(S_3)\mathcal{L}_{min}(S_6),\mathcal{L}(S_1)\mathcal{L}_{min}(S_6)),$$

де $\mathcal{L}_{min}(F) = \min_{b\in F_2^n, b\neq 0}\ max_{a\in F_2^n}|\lambda_F(a,b)|$
Більш того,

1) Якщо S_4 та S_5 – бієктивні, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_4)\mathcal{L}_{min}(S_5^{-1})$$

2) Якщо S_2 та S_5 – бієктивні, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_2)\mathcal{L}_{min}(S_5^{-1})$$

3) Якщо S_3 – бієктивний, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_3)\mathcal{L}_{min}(S_6^{-1})$$

4) Якщо S_1 та S_6 – бієктивні, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_1)\mathcal{L}_{min}(S_6^{-1})$$

Доведення. Даний результат є прямим наслідком Теореми 2.3. Так само, як в Теоремі 2.2 обираємо найкращі лінійні потенціали та оцінюємо їх. Розглянемо пару масок (α,β), на якій деяке S_i досягає нелінійності: $\mathcal{L}(S_i)$. Для $i = 4$ або $i = 5$ з першого випадку Теореми 2.3 отримаємо для будь-якого γ:

$$|\lambda_F(0||0||0||\alpha,\beta||\alpha||\alpha||\gamma)| = \mathcal{L}(S_4) \times |\lambda_{S_5}(\alpha,\beta \oplus \gamma)|$$
$$|\lambda_F(0||0||0||\alpha,\beta \oplus \gamma||\alpha||\alpha||\gamma)| = \mathcal{L}(S_5) \times |\lambda_{S_4}(\alpha,\beta \oplus \gamma)|$$

Тоді, для зазначених вище випадків обираємо ненульве значення γ та θ, що максимізує перетворення Уолша для правої компоненти рівняння. За визначенняи, $\mathcal{L}_{min}(S_j)$ тоді є нижньою оцінкою для перетворення Уолша, що знаходиться з правої частини рівняння.

Останній пункт теореми доводиться з використанням другої та третьої частини Теореми 2.3. Для будь-якого γ отримаємо

$$|\lambda_F(0 \parallel \alpha \parallel 0 \parallel 0, \alpha \parallel \gamma \parallel \beta \parallel \alpha)| = \mathcal{L}(S_3) \times |\lambda_{S_6}(\alpha, \beta \oplus \gamma)|$$
$$|\lambda_F(\alpha \parallel 0 \parallel 0 \parallel 0, \beta \parallel \gamma \parallel 0 \parallel \beta)| = \mathcal{L}(S_1) \times |\lambda_{S_6}(\beta,\gamma)|$$

Тоді, якщо S_6 є перестановкою , для будь-якого фіксованого $\alpha \neq 0$

$$\max_{\gamma \in F_2^n} |\lambda_{S_6}(\alpha,\gamma)| \geq \mathcal{L}_{min}(S_6^{-1}).$$

Аналагічно отримано, якщо S_5 є перестановкою , для будь-якого фіксованого $\alpha \neq 0$:

$$\max_{\gamma \in F_2^n} |\lambda_{S_5}(\alpha,\gamma)| \geq \mathcal{L}_{min}(S_5^{-1}).$$

2.3 Порівняння криптографічних властивостей схеми CLEFIA з іншими схемами безключових перетворень

У своїй роботі [1] Лі та Ванг одержали аналітичні оцінки для диференціальної рівномірності та лінійних потенціалів для трираундової безключової схеми Фейстеля. А.Канто та ін. [2] покращили ці оцінки та поширили їх на трираундову схему MISTY. Після цього у бакалаврській роботі було отримано оцінки на трираундову R-схему.

У даному розділі проводиться порівняльний аналіз отриманих оцінок для трираундової безключової схеми CLEFIA з оцінками для трираундової безключової схеми MISTY, отриманими у роботі А.Канто та ін. [2], та покращеними ними оцінками для трираундової безключової схеми Фейстеля,отриманих у роботі Лі та Ванга [1], та отриманими раніше у бакалаврській дипломній роботі оцінками для трираундової безключової R-схеми.

Спочатку наведемо загальні оцінки для диференціальної однорідності та лінійних потенціалів трираундової безключової схеми Фейстеля, трираундової безключової схеми MISTY, трираундової безключової R-схеми, та трираундової безключової схеми CLEFIA.

Трираундова схема Фейстеля

Диференціальна однорідність

$$\delta(F) \geq \delta(S_2)\max(\delta_{min}(S_1),\delta_{min}(S_3))$$

1) Якщо S_2 – не є перестановкою, то

$$\delta(F) \geq 2^{n+1}$$

2) Якщо S_2 – перестановка, то

$$\delta(F) \geq \max_{i\neq 2, j\neq 2, i} \max(\delta(S_i)\delta_{min}(S_j), \delta(S_i)\delta_{min}(S_2^{-1})))$$

Лінійні потенціали

$$\mathcal{L}(F) \geq \mathcal{L}(S_2) \max(\mathcal{L}_{min}(S_1), \mathcal{L}_{min}(S_3))$$

1) Якщо S_2 – перестановка, то

$$\mathcal{L}(F) \geq \max_{i\neq 2, j\neq 2, i} \max(\mathcal{L}(S_i)\mathcal{L}_{min}(S_j), \mathcal{L}(S_i)\mathcal{L}_{min}(S_2^{-1})))$$

Трираундова схема MISTY

Диференціальна однорідність

$$\delta(F) \geq \delta(S_1) \max(\delta_{min}(S_2), \delta_{min}(S_3))$$

1) Якщо S_1 – не є перестановкою, то

$$\delta(F) \geq 2^{n+1}$$

2) Якщо S_1 – перестановка, то

$$\delta(F) \geq \max_{i\neq 1, j\neq 1, i} \max(\delta(S_i)\delta_{min}(S_j), \delta(S_i)\delta_{min}(S_1^{-1})))$$

Лінійні потенціали

$$\mathcal{L}(F) \geq \max(\mathcal{L}(S_1)\mathcal{L}_{min}(S_2), \mathcal{L}(S_2)\mathcal{L}_{min}(S_1), \mathcal{L}(S_3)\mathcal{L}_{min}(S_1))$$

1) Якщо S_3 – перестановка, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_1)\mathcal{L}_{min}(S_3^{-1})$$

2) Якщо S_1 – перестановка, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_3)\mathcal{L}_{min}(S_2)$$

3) Якщо S_1 та S_3 – перестановки, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_2)\mathcal{L}_{min}(S_3^{-1})$$

Трираундова R-схема

Диференціальна однорідність

$$\delta(F) \geq \delta(S_1)\max(\delta\min(S_3), \delta\min(S_2)),$$

1) якщо S_1 є перестановкою:

$$\delta(F) \geq \max_{i\neq 1, j\neq 1, i} \max(\delta(S_i)\delta_{min}(S_j), \delta(S_i)\delta_{min}(S_1^{-1})),$$

2) якщо S_1 не є перестановкою:

$$\delta(F) \geq 2^{n+1}.$$

Лінійні потенціали

$$\mathcal{L}(F) \geq \max(\mathcal{L}(S_1)\mathcal{L}_{min}(S_2), \mathcal{L}(S_2)\mathcal{L}_{min}(S_1), \mathcal{L}(S_3)\mathcal{L}_{min}(S_1)),$$

1) Якщо S_1 та S_2 – перестановки, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_2)\mathcal{L}_{min}(S_3)$$

2) Якщо S_1 та S_2 – перестановки, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_3)\mathcal{L}_{min}(S_1^{-1})$$

3) Якщо S_1 – перестановка, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_2)\mathcal{L}_{min}(S_1^{-1})$$

Трираундова схема CLEFIA

Диференціальна однорідність

$$\delta(F) \geq \max(\delta(S_6)\delta\min(S_4), \delta(S_5)\delta\min(S_3)),$$

1) Зокрема, якщо S_6 є перестановкою:

$$\delta(F) \geq \max_{i\neq 6, j\neq 6, i} \max(\delta(S_i)\delta_{min}(S_j), \delta(S_{i+1})\delta_{min}(S_6^{-1})),$$

2) якщо S_4 не є перестановкою:

$$\delta(F) \geq 2^{n+1}.$$

Лінійні потенціали

$$\mathcal{L}(F) \geq \max(\mathcal{L}(S_4)\mathcal{L}_{min}(S_5), \mathcal{L}(S_2)\mathcal{L}_{min}(S_5), \mathcal{L}(S_3)\mathcal{L}_{min}(S_6), \mathcal{L}(S_1)\mathcal{L}_{min}(S_6)),$$

1) Якщо S_4 та S_5 – бієктивні, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_4)\mathcal{L}_{min}(S_5^{-1})$$

2) Якщо S_2 та S_5 – бієктивні, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_2)\mathcal{L}_{min}(S_5^{-1})$$

3) Якщо S_3 – бієктивний, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_3)\mathcal{L}_{min}(S_6^{-1})$$

4) Якщо S_1 та S_6 – бієктивні, то

$$\mathcal{L}(F) \geq \mathcal{L}(S_1)\mathcal{L}_{min}(S_6^{-1})$$

У роботі [2] проаналізовано криптографічні властивості 8-бітових S-блоків, побудованих за трираундовою безключовою схемою Фейстеля, та S-блоків, побудованих за трираундовою безключовою схемою MISTY. У бакалаврській дипломній роботі проаналізовано криптографічні властивості 8-бітових S-блоків, побудованих за трираундовою безключовою R-схемою.

Проаналізуємо криптографічні властивості 16-бітових S-блоків побудованих за трираундовою безключовою схемою CLEFIA з 4-бітними внутрішніми S-блоками, з особливим акцентом на тому випадку, коли три внутрішніх S-блоки є бієкціями, так як це відповідає випадку, коли отримана функція є перестановкою.

Зокрема, для будь-якого 4-бітної функції S, $\delta_{min}(S) \geq 2$ і $\mathcal{L}_{min}(S) \geq 4$. Більш того, якщо S – це 4-бітова перестановка, то $\delta_{min}(S) \geq 4$ і $\mathcal{L}_{min}(S) \geq 8$.

Наступна оцінка для диференціальної рівномірності трираундової схеми CLEFIA над F_2^{16} є прямим наслідком Теореми 2.2.

Лема 2.1. *Будь-яка 16-бітна функція F, побудована за структурою трираундової схеми CLEFIA із відображеннями S_1, S_2, S_3, S_4, S_5, та S_6 в якості раундових перетворень, досягає $\delta(F) \geq 8$.*

Доведення. Оцінка явно має місце коли S_4 не є бієкцією, так як відомо з Теореми 2.2, що в цьому випадку $\delta(F) \geq 2^5 = 32$. Якщо S_4 – бієкція, то $\delta(S_4) \geq 4$, так як APN перестановки над F_2^4 не існують. Очевидно, що будь-який 4-бітний S-блок S задовольняє $\delta_{min}(S) \geq 2$, це означає, що

$$\delta(F) \geq \delta(S_4)\delta_{min}(S_6) \geq 8$$

□

Крім цього загального результату, можна забезпечити деякі необхідні умови на S-блок для досягнення попередньої нижньої оцінки. Цей результат заснований на наступній лемі.

Лема 2.2. *Нехай S_4 є 4-бітовою пересановкою з $\delta(S_4) = 4$ і S_1, S_2, S_3, S_5 та S_6 є 4-бітовими функціями. Нехай F – це 16-бітова функція, побудована за структурою трираундової схеми CLEFIA із відображеннями S_1, S_2, S_3, S_4, S_5, та S_6 в якості раундових перетворень. Якщо $\delta(S_5) \geq 4$ або $\delta(S_6) \geq 4$ або $\delta(S_3) \geq 4$, тоді $\delta(F) \geq 16$*

Доведення. Нехай позначимо через $\mathcal{C}(S)$ безліч стовпців в таблиці розподілів диференціалів S-блоку, який складається тільки з $0s$ і $2s$. Після чого, з першої частини Теореми 2.1 слідує, що $\delta(F) \geq 16$, хоча $\mathcal{C}(S_4)$ містить всі рядки з таблиці розподілів диференціалів S_6 зі значенням більшим чи рівним 4. Крім того, з другої частини Теореми 2.1 слідує, що $\delta(F) \geq 16$, хоча $\mathcal{C}(S_3)$ містить всі рядки в таблиці різниці S_5 з 4. Така ситуація неможлива. □

Таким чином, отримано наступну умову для побудови трираундової схеми CLEFIA над F_2^{16} з диференціальною рівномірністю рівною 8.

Теорема 2.5. *Нехай S_1, S_2, S_3, S_4, S_5 та S_6 є трьома 4-бітними S-блоками та нехай F – це 16-бітова функція, побудована за структурою трираундової схеми CLEFIA із відображеннями S_1, S_2, S_3, S_4, S_5 та S_6 в якості раундових перетворень. Тоді $\delta(F) = 8$ означає, що S_4 є перестановкою з $\delta(S_4) = 4$ та S_3, S_4 і S_6 є APN функціями. В іншому випадку $\delta(F) \geq 12$*

Доведення. Так як $\delta(F) \geq 32$ виконується, коли S_4 не є бієкцією, необхідно зосередитися на тому випадку, коли S_4 є перестановкою.

Якщо який-небудь із складових S-блоку S_i має диференціальну рівномірність строго більше ніж 4, тобто, $\delta(S_i) \geq 6$, з Теореми 2.2 випливає, що $\delta(F) \geq \delta(S_i)\delta_{min}(S_j) \geq 12$. Таким чином, $\delta(F) = 8$ може бути досягнута тільки тоді, коли $\delta(S_4) = 4$, $\delta(S_3) \leq 4$, $\delta(S_5) \leq 4$ і $\delta(S_6) \leq 4$. Той факт, що $\delta(F) \geq 16$, коли хоча б один з S-блоків S_3, S_5 або

S_6 має диференціальну рівномірність 4, доведено в Лемі 2.2. □

Теорема 2.6. *Нехай S_1, S_2, S_3, S_4, S_5 та S_6 є трьома 4-бітними S-блоками та нехай F – це 16-бітова функція, побудована за структурою трираундової схеми CLEFIA із відображеннями S_1, S_2, S_3, S_4, S_5 та S_6 в якості раундових перетворень. Тоді $\delta(F) \geq 16$.*

Доведення. Результат є прямим наслідком Теореми 2.1. Дійсно, гарантовано існують такі a, b і c, що щонайменше одна з наступних трьох властивостей виконується:

1) $\delta_{S_4}(a, b) \geq 4$ та $\delta_{S_6}(b, c) \geq 4$.

2) $\delta_{S_3}(a, b) \geq 4$ та $\delta_{S_5}(b, c) \geq 4$.

У кожному з цих випадків, Теорема 2.1 має диференціал (α, β) для F з $\delta_F(\alpha, \beta) = 16$ □

Використовуючи факт, що будь-яка 4-бітова перестановка S задовольняє умові $\mathcal{L}(S) \geq 8$ і $\mathcal{L}_{min} \geq 8$, виводимо безпосередньо з Теореми 2.4 наступні оцінки.

Теорема 2.7. *Нехай S_1, S_2, S_3, S_4, S_5 та S_6 є трьома 4-бітними S-блоками та нехай F – це 16-бітова функція, побудована за структурою трираундової схеми CLEFIA із відображеннями S_1, S_2, S_3, S_4, S_5 та S_6 в якості раундових перетворень. Якщо який-небудь з шести внутрішніх S-блоків є перестановкою, то*

$$\mathcal{L}(F) \geq 64$$

Більш того, якщо $\mathcal{L}(F) < 64$ то $\delta(F) \geq 32$

Навіть якщо трираундова схема CLEFIA має $\mathcal{L}(F) < 64$, можна показати, що її лінійність складає щонайменше 48.

Теорема 2.8. *Нехай S_1, S_2, S_3, S_4, S_5 та S_6 є трьома 4-бітними S-блоками та нехай F – це 16-бітова функція, побудована за структурою трираундової схеми CLEFIA із відображеннями S_1, S_2, S_3, S_4, S_5 та S_6*

в якості раундових перетворень. Тоді

$$\mathcal{L}(F) \geq 48$$

Доведення. Теорема 2.4 показує, що результат має місце, якщо S_6 є перестановкою. Припустимо, що S_6 не є перестановкою, тобто існує деяка ненульова вихідна маска c, така що $\lambda_{S_6}(,0) > 0$. Використовуючи четвертий пункт Теореми 2.3, отримуємо, що

$$\lambda_F(a \parallel 0 \parallel 0 \parallel 0, 0 \parallel c \parallel 0 \parallel 0) = \lambda_{S_1}(a,0) \times \lambda_{S_6}(0,0) = 16\lambda_{S_3}(a,c)$$

Отриманий результат має місце, якщо існує деяка ненульова a, така що $\lambda_{S_1}(a,0) \geq 4$. В іншому випадку випливає, що

$$\mathcal{L}(F) \geq 48$$

□

Найкращі результати, що можна досягти для 8-бітного оборотного S-блоку, є:

1) для трираундової схеми Фейстеля: $\delta(F) = 8$ і $\mathcal{L}(F) = 64$.

2) для трираундової схеми MISTY: $\delta(F) = 16$ і $\mathcal{L}(F) = 64$.

3) для трираундової R-схеми: $\delta(F) = 16$ і $\mathcal{L}(F) = 64$.

4) для трираундової схеми CLEFIA: $\delta(F) = 16$ і $\mathcal{L}(F) = 64$.

Якщо $n = 4$, для чотирьох конструкцій виконується:

$$\delta(F) \geq 8,$$
$$\mathcal{L}(F) \geq 48.$$

Крім того, $\mathcal{L}(F) \geq 64$, якщо $\delta(F) \geq 32$.

Для побудови схем R-схеми та схеми CLEFIA з $n = 4$, якщо F є

перестановкою, отримано більш жорсткі оцінки:

$$\delta(F) \geq 16,$$
$$\mathcal{L}(F) \geq 64.$$

Варто зауважити, що ці результати пояснюють порівнювані властивості S-блоків, отриманих за допомогою моделювання, запропонованого в роботі [25]. Отримані результати усіх структур дуже схожі, але для безключової схеми CLEFIA та безключової R-схеми оптимальні результати досягаються тільки при необоротних внутрішніх функціях та накладанні умов на блоки. Це означає, що схема Фейстеля є більш придатною для побудови 8-бітових або 16-бітових перестановок.

Таким чином, дана робота показує, що трираундова безключова схема Фейстеля дозволяє отримати кращі результати, ніж трираундова безключова схема MISTY, трираундова безключова R-схема та трираундова безключова схема CLEFIA для проектування оборотних 8-бітових або 16-бітових S-блоків.

Однак, в деяких інших контекстах трираундова безключова схема CLEFIA та трираундова безключова R-схема мають ряд переваг, оскільки вони забезпечують більш високу продуктивність з точки зору пропускної здатності і час очікування через перші два S-блоків для R-схеми та чотири S-блоки для схеми CLEFIA може бути оцінений паралельно.

Висновки до розділу 2

У даному розділі одержано аналітичні оцінки для диференціальної рівномірності та лінійних потенціалів безключової схеми CLEFIA, виражені через відповідні параметри її раундових перетворень (S-блоків). Отримані оцінки криптографічних властивостей схем безключового

перетворення можуть використовуватись на практиці для створення нових шифрів підвищеної надійності.

На основі проведених досліджень зроблено порівняльний аналіз криптографічних схем безключових перетворень. Зокрема, доведено, що схема Фейстеля переважає схему CLEFIA у випадку побудови 8-бітових або 16-бітових перестановок.

ВИСНОВКИ

Дана робота становить собою закінчене наукове дослідження, присвячене вирішенню актуальної наукової задачі теоретичного оцінювання стійкості безключових схем блокових перетворень до диференціального та лінійного криптоаналізу. Проведені дослідження дозволили отримати нові наукові результати, перелічені нижче.

1) На основі проведеного аналізу встановлено, що сучасні криптографічні методи захисту інформації в приладах з обмеженою обчислювальною потужністю, малим об'ємом пам'яті та малим енергоспоживання вимагають знаходження нових та переробки вже існуючих схем криптографічних перетворень.

2) На основі проведеного аналізу встановлено, що для вивчення криптографічних властивостей схем ітеративних безключових перетворень для побудови легких S-блоків, необхідно вивчити ці схеми з фіксованим ключем, так як схема з фіксованим ключем еквівалентна схемі криптографічних перетворень без ключа з різними S-блоками.

3) Одержано аналітичні оцінки диференціальної рівномірності для трираундової безключової схеми CLEFIA через відповідні параметри її раундових функцій. Отримані результати позволяють підвищити ефективність методів аналізу та синтезу алгоритмів легкої криптографії.

4) Одержано аналітичні оцінки лінійних потенціалів для трираундової безключової схеми CLEFIA через відповідні параметри її раундових функцій. За результатами проведеного аналізу рекомендовано використовувати схему CLEFIA блокового перетворення для синтезу блокових шифрів легкої криптографії як внутрішню нелінійну функцію.

5) На основі проведених досліджень зроблено порівняльний аналіз криптографічних схем безключових перетворень. Цікаво відзначити, що трираундова безключова схема CLEFIA не може запропонувати такий же рівень безпеки, як схема Фейстеля для побудови оборотних 8-бітних

S-блоків. Сфера застосування отриманих результатів включає як аналіз вже існуючих шифрів та проектів шифрів легкої криптографії (у тому числі таких, що використовуються в діючих системах криптографічного захисту інформації), так і створення нових, доказово захищених алгоритмів шифрування легкої криптографії. Таким чином, дана робота сприяє підвищенню рівня та якості сучасної інформаційної безпеки.

6) На основі отриманих оцінок криптографічних властивостей схем безключового перетворення у подальшому будуть проведені розробки конкретного 16-бітного оборотного S-блоку, оптимізованого для легквагової реалізації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Li Y. Constructing S-boxes for Lightweight Cryptography with Feistel Structure / Li Y., Wang // Cryptographic Hardware and Embedded Systems. – 2014.

2. Canteaut A. Construction of Lightweight S-Boxes using Feistel and MISTY structures (Full Version) [електронний ресурс] / Anne Canteaut, Sebastien Duval, Gaetan Leurent // – 2015. – Режим доступу: http://eprint.iacr.org/2015/711.pdf.

3. Matsui M. Linear cryptanalysis method for DES cipher. / Matsui M. // Advances in Cryptology. – EUROCRYPT'93. – LNCS, – vol. 765, – pp. 386–397, – Springer (1994)

4. Biham E. Differential Cryptanalysis of DES-like Cryptosystems / Biham E., Shamir A. // Journal of Cryptology. – 1991.–V.4.–№1.–P.3–72.

5. Heys Howard M. A Tutorial on Linear and Differential Cryptanalysis [електронний ресурс] / Heys Howard M. // – Режим доступу: http://www.engr.mun.ca/ howard/PAPERS/ldc$_t$*utorial.pdf*

6. Nyberg K. PRESENT: An Ultra-Lightweight Block Cipher. / K. Nyberg // – Advances in Cryptology - Proceedings of Eurocrypt '91. – Lecture Notes in Computer Science 547, Springer Verlag, 1991 – pp. 378-386

7. Bogdanov A. Perfect nonlinear S-boxes / Bogdanov A., Knudsen L.R., Leander G., Paar C., Poschmann A., Robshaw M.J.B., Seurin Y., Vikkelsoe C. // – CHES 2007, – LNCS, – vol. 4727, – pp. 450-466, – Springer, 2007

8. Hong D. HIGHT: A New Block Cipher Suitable for Low-Resource Device / Hong D., Sung J., Hong S., Lim J., Lee S., Koo B., Lee C., Chang D., Lee J., Jeong K., Kim H., Kim J., Chee S. // – CHES 2006, – LNCS, – vol. 4249, – pp. 46-59, – 2006

9. Wu W. LBlock: Lightweight Block Cipher. [електронний ресурс] / Wu W., Zhang L. // – Cryptology ePrint Archive, – Report 2011/345 – Режим доступу: http://eprint.iacr.org

10. Suzaki T. Twine: A Lightweight, Versatile Blockcipher. [електронний ресурс] / Suzaki T., Minematsu K., Morioka S., Kobayashi E. // – 2011. – ECRYPT Workshop on Lightweight Cryptography – Режим доступу: http://www.uclouvain.be/crypto/ecrypt lc11/static/post proceedings.pdf. 2011

11. Beaulieu R. The SIMON and SPECK Families of Lightweight Block Ciphers. [електронний ресурс] / Beaulieu R., Shors D., Smith J., Clark S.T., Weeks B., Wingers L. // – Cryptology ePrint Archive, – Report 2013/404 – Режим доступу: http://eprint.iacr.org

12. Leander G. New Lightweight DES Variants. / Leander G., Paar C., Poschmann A.// – FSE 2007, – LNCS, – vol. 4593, – pp. 196-210, – 2007

13. Shirai T. The 128-bit Block cipher CLEFIA (Extended Abstract) / Shirai T., Shibutani K., Akishita T., Moriai S., Iwata T.// – FSE 2007, – LNCS, – vol. 4593, – pp. 181-195, – 2007

14. Cannire C. Katan and Ktantana family of small and efficient hardware-oriented block ciphers / Cannire C., Dunkelman O., Knezevi M.// – CHES 2009, – LNCS, – vol. 5747, – pp.272-288, – 2009

15. Hell M. Grain : a Stream Cipher for Constrained Environments. / Martin Hell, Thomas Johansson, and Willi Meier.// –Int. J. Wire. Mob. Comput., – 2(1):86–93, – May 2007.

16. Babbage S. The stream cipher MICKEY 2.0 [електронний ресурс] / Steve Babbage and Matthew Dodd // – 2006. – Режим доступу: http://www.ecrypt.eu.org/stream/mickeypf.html

17. Tian Y. On the Design of Trivium. [електронний ресурс] / Yun Tian, Gongliang Chen, and Jianhua Li. // – Cryptology ePrint Archive, – Report 2009/431, – 2009. – Режим доступу: http://eprint.iacr.org/

18. Daemen J. The Design of Rijndael: AES - The Advanced Encryption Standard. / Joan Daemen and Vincent Rijmen. // – Information Security and Cryptography.– Springer,– 2002.

19. Lim C.H. CRYPTON: A New 128-bit Block Cipher / Lim C.H. // – AES submission. – 1998

20. Lim C.H. A Revised Version of CRYPTON - CRYPTON V1.0. / Lim C.H. // – Fast Software Encryption – FSE'99. – LNCS, – vol. 1636, – pp. 31–45. – Springer (1999)

21. Barreto P.S. The WHIRLPOOL Hashing Function. /Barreto P.S., Rijmen V. // – NESSIE submission

22. Barreto P.S. The KHAZAD Legacy-Level Block Cipher. /Barreto P.S., Rijmen V. // – NESSIE submission

23. Standaert F. ICEBERG : An involutional cipher efficient for block encryption in reconfigurable hardware. /Standaert F., Piret G., Rouvroy G., Quisquater J., Legat J.// – Fast Software Encryption - FSE 2004. – LNCS, – vol. 3017, – pp. 279–299. – Springer (2004)

24. Gerard B. Block ciphers that are easier to mask: How far can we go? / Gerard B., Grosso V., Naya-Plasencia M., Standaert F.// – Cryptographic Hardware and Embedded Systems - CHES 2013. – LNCS, – vol. 8086, – pp.383–399. – Springer (2013)

25. Grosso V. LS-designs: Bitslice encryption for efficient masked software implementations. / Grosso V., Leurent G., Standaert F.X., Varıcı K.// – Fast Software Encryption - FSE 2014. – LNCS, – Springer (2014)

26. Usman M. SIT: A Lightweight Encryption Algorithm for Secure Internet of Things [електронний ресурс] / Muhammad Usman, Irfan Ahmed, M. Imran Aslam, Shujaat Khan, Usman Ali Shah // – 2017. – Режим доступу: https://arxiv.org/pdf/1704.08688.pdf.

27. Toshihiko O. Lightweight Cryptography Applicable to Various IoT Devices [електронний ресурс] / Okamura Toshihiko // – 2017. – Режим доступу: https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html

28. Современные направления развития криптографических методов защиты информации [електронний ресурс] / Биккулов А.Х. // – 2017. – Режим доступу: https://scienceforum.ru/2017/article/2017033579

29. Poschmann A. Y. LIGHTWEIGHT CRYPTOGRAPHY Cryptographic Engineering for a Pervasive World [електронний

ресурс] / Axel York Poschmann // – 2009. – Режим доступу: https://eprint.iacr.org/2009/516.pdf

30. CRYPTREC Cryptographic Technology Guideline (Lightweight Cryptography) [електронний ресурс] / National Institute Of Information And Communications Technology // – 2017. – Режим доступу: https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016en.pdf

31. Yevsyukova Y. Estimations of Differential Probabilities of Unkeyed R-Scheme of Block Encryption [електронний ресурс] / Yana Yevsyukova, Serhii Yakovliev // – 2017. – Режим доступу: http://itcm.comp-sc.if.ua/2017/Yevsyukova.pdf

32. Nyberg K. Generalized Feistel networks [електронний ресурс] / Kaisa Nyberg // – 2005. – Режим доступу: https://link.springer.com/chapter/10.1007/BFb0034838

33. Schneier B. Unbalanced Feistel Networks and Block-Cipher Design [електронний ресурс] / Bruce Schneier, John Kelsey // – 2018. – Режим доступу: https://www.schneier.com/academic/paperfiles/paper-unbalanced-feistel.pdf

34. Choy J. Cryptographic Properties and Application of a Generalized Unbalanced Feistel Network Structure (Revised Version) [електронний ресурс] / Jiali Choy, Guanhan Chew, Khoongming Khoo, Huihui Yap // – 2009. – Режим доступу: https://eprint.iacr.org/2009/178.pdf

35. Rebeiro C. Differential Cache Trace Attack Against CLEFIA [електронний ресурс] / Chester Rebeiro, Debdeep Mukhopadhyay // – 2010. – Режим доступу: https://https://eprint.iacr.org/2010/012.pdf

36. Boura C. Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon (Full Version) [електронний ресурс] / Christina Boura, Maria Naya-Plasencia, Valentin Suder // – 2014. – Режим доступу: https://eprint.iacr.org/2014/699.pdf